數　論

J. W. A. Young 著

王雲五主編

萬有文庫

第一集一千種

數論尺規作圖及周率

楊氏 狄克孫 斯密斯著

鄭太朴譯

上海寶山路
商務印書館　　發行兼印刷者

上海及各埠
商務印書館　　發行所

中華民國十九年十月初版

T

Y. W. W

THEO[illegible] NUMBERS, by J. W. [illegible] YOUNG
CONSTRUCTION WITH RU[illegible] COMPASS
by L. E. DICKSON
HISTORY OF π, by DAVID EUGENE SMITH
Translated by
CHÊNG T'AI P'O

THE COMMERCIAL PRESS, LTD.
Shanghai, China
1930

目　次

數　　論

J. W. A. Young 著

目　　次

數　論

J. W. A. Young 著

I. 引　言

1. 在某種意義上說來，"數目論" 直可將數學上尋常所研究的一切對象一齊包括進去，蓋除了幾何學中之無度量的部分外，數學上其餘諸部分鮮有不是根本上與數目有關者。但此語之意義，尋常限於表"整"數目（正，負，零）之理論。惟於此還須加限制，蓋整數以外之其他數目，可用整數定其意義（參觀第四篇附錄一），故研究建設於整數上之全部理論，仍將研究及差不多全部數學。於是尋常限制"數目論"爲關於整數之"如

是"者，其屬性及用運算法連結之的結果亦是整的。故可許用加，減，乘於任何整數，而除則祇許用於整數其商爲整者。除亦可用以求整數間之方程。例如 $9385=62\cdot151+23$（註：數目間之點卽爲乘號）。

故凡下面用"數目"一語，所指者是"整數"；而其他用語，如"因子"，其意義亦如是限制。

2. 如是限制好的對象，若正則研究之，似當開首時先一論整數概念之性質與發生，關於整數及用入的運算法之根本定義與目題（*postulate*）以及運算"定律"，等等。但此則至於某程度乃是研究初等算術之理論的基礎了。

3. 這裏假定一些初等算術之智識，而開始卽研究各種屬性，與數目之因子相連，爲尋常彼中所不論及者。

II. 因子

4. 定義 一數目除其本身及一以外沒有其他

因子者，為質數。

5. 定理　質數有無限多。

〔證〕 我們祇須證明，能有一質數較之任何已知的質數為大，今設已知的質數為 p。則試論

$$N=2\cdot3\cdot5\cdots p+1,$$

於此 N 之首項為一切不大於 p 的質數之積。由此 N 之式，可見倘 N 為適纔所說任何一質數所除，總餘一。故知 N 之每一質因子必大於 p。因 N 必有一或多於一的質因子，故已證明可有一大於 p 的質數"存在。"然此與"實際上求得"一大於一已知的質數 p 的質數不同。倘沒有發見普通求之的方法。

此定理亦可如是說法：不能有最大的質數；或說：將質數依其大之次序排列之，每質數後必繼之以他質數；或亦可說：質數之數無限。這種種說法均同。

會猜想過每一偶數乃是二質數之和，惟未經證明。

6. 前述的定理二千年前歐几里得(*Euclid*)已知之。十九世紀時，狄利希萊(*Dirichlet*)將其擴充爲：每一算術級數其首項與公差無公因子者，其內含有無限數的質數。

狄氏之證，所用數目及運算法非這裏所許者，(參觀前1節)，但由此可知算術上的命題有可用“非算術的”證以明之者。

於某幾種級數，此定理極易算術的證明之。例如級數

$$3,7,11,15,19,23,\cdots 4n-1,\cdots$$

含有無限數的質數之相續。欲證明此，祗須指出對於每一質素p，能有一較大的質數作$4n-1$形式者存在。試一論

$$N=2(2\cdot 3\cdot 5\cdot 7\cdots p)-1,$$

於此括弧中之數乃是一切不大於p的質數之積。由此N之形式可知$2,3,\cdots p$等諸質數均非N之因子，故N之一切質因子必大於p。

凡奇質數之形式爲$4n+1$或$4n-1$。二數目作

$4n+1$ 形式者，其積亦爲 $4n+1$ 形式。但 N 之形式爲 $4n-1$，故至少其一質因子的形式必爲 $4n-1$。如是，已證明能有一質數作此形式者大於 p 存在。

仿此可證明以下級數含有無限數的質數：

$$5,11,17,23,29,35\cdots,6n-1,\cdots$$

7. 關於質數，曾有許多重要普通問題已研究過。例如

(1) 決定一間隙(*interval*)內所有質數之數目。

(2) 決定一大於一已知質數的質數。

(3) 決定一質數，次大於一已知的質數者。

(4) 決定一已知的數目是否是質數；或廣之，決定一已知數之因子。

這些問題均尚未有普通的解決。

8. 求因子之最簡的方法，祗有去試驗。但祗須用質數試驗，而此中，祗須其平方小於已知的數者。於大的數目，此法殊不便。於此，數目論中所得結果與方法有許多可用。

9．一千萬以下的因子表已有出版。維也納(*Vienna*)學院叢集中有稿本，內載3,000,000,至100,000,000 各數目之因子（此稿中已知有許多錯誤）。

10．特殊的數目較表中所載更大者，其因子亦已有求得。例如有法多角形作法理論（參觀第八篇 26 節）中，極須要知道 $2^{2^n}+1$ 是否一質數。已明白

$$2^{2^5}+1=4,294,967,297$$
$$=641\cdot6,700,417。$$

還有一數目多於二十萬兆位者，$2^{2^{36}}+1$，其質因子爲

$$2,748,779,069,441。$$

11．定義　二數目除一以外無公因子者爲“互質。”每個對於其他爲質數。

12．定義　不大於m而對於m爲質的正整數之數，名爲m之“質總”(*totient*)，用$\phi(m)$表之。如是，

$$\phi(1)=1;\ \phi(2)=1;\ \phi(3)=2;\ \phi(4)=2;$$

$$\phi(5)=4;\ \phi(6)=2;\ \phi(7)=6;\ \phi(8)=4。$$

設p爲質數，　　$\phi(p)=p-1$。

13. 問題　試決定$\phi(m)$。

〔解法〕設 $m=p^aq^br^c\cdots v^h$，於此 $p,q,r,\cdots v$ 爲不同的質數，$a,b,c,\cdots h$ 爲正整數。設由這一級數目

$$1,2,3,4,5,\cdots m-1,m,$$

中將其有 p 或 q 或 r 等爲因子的各數目剔出，則所餘數目對於m自卽爲質的，而其數目卽是所求的質總。

試先論其有 p 爲因子者。這些是 $p,2p,3p,\cdots \frac{m}{p}\cdot p$。其數目爲$\frac{m}{p}$(註：這 $\frac{m}{p}$ 是一整數，因p爲m之因子。仿此，以後凡用分數式表出的數目亦是整的)。因之，此數目級中無 p 爲因子的數目，當有$m-\frac{m}{p}$或$m\left(1-\frac{1}{p}\right)$個。廣言之，可如是說：

補題　設M有質因子p，則$1,\ 2,\ 3,\cdots M$中無

p 爲因子之數目共有 $M\left(1-\frac{1}{p}\right)$ 個。

其次再剔去有 q 爲因子的數目。這些是 $q, 2q, \cdots \frac{m}{q}\cdot q$。其中或者有的因有 p 爲因子，已經剔去。其無有 p 爲因子者之數目，乃是無有 p 爲因子的係數 $1,2,3,\cdots\frac{m}{q}$ 之數目。照補題，可知此數目是 $\frac{m}{q}\left(1-\frac{1}{p}\right)$。如是，$1,2,3,\cdots m$ 中無有 p 與 q 爲因子的數目，其數爲

$$m\left(1-\frac{1}{p}\right)-\frac{m}{q}\left(1-\frac{1}{p}\right)$$

或
$$m\left(1-\frac{1}{p}\right)\left(1-\frac{1}{q}\right)$$

仿此，$r, 2r, 3r, \cdots\frac{m}{r}\cdot r$ 諸數有 r 爲因子。其中或者有以 p 與 q 爲因子者。至其沒有者之數，則是無有 p 與 q 爲因子的係數卽 $1,2,3,\cdots\frac{m}{r}$ 之數。由前面結果，此數是 $\frac{m}{r}\left(1-\frac{1}{p}\right)\left(1-\frac{1}{q}\right)$。故 $1, 2, 3, \cdots m$ 中所有不能用 p, q, r 除的數目，其數爲

$$m\left(1-\frac{1}{p}\right)\left(1-\frac{1}{q}\right)-\frac{m}{r}\left(1-\frac{1}{p}\right)\left(1-\frac{1}{q}\right)$$

或　　$$m\left(1-\frac{1}{p}\right)\left(1-\frac{1}{q}\right)\left(1-\frac{1}{r}\right)。$$

此方法，可推及m之一切質因子。於是所餘者與m爲互質數故得

$$\phi(m)=m\left(1-\frac{1}{p}\right)\left(1-\frac{1}{q}\right)\left(1-\frac{1}{r}\right)\cdots\left(1-\frac{1}{v}\right)。$$

〔附識〕(1)尋常用"數學的歸納法"以推論至於m之一切質因子，卽是，凡如前一種結果適用於任何k個m之不同的質因子，此項結果於m之$k+1$個質因子亦適用，卽已論過的k個上加一。因此項結果於一，二，三個因子已證明，故於四個因子亦可用，於是五個，六個等均可用，而推及至於一切因子。

(2) 倘讀者於普通的m感有困難，則可先從事一二個特例，如 $60=2^2\cdot3\cdot5$，$48=2^4\cdot3$，$55=5\cdot11$ 等，然後推廣之。其他處所亦可如此。若不多從事於特例工作，必不能學好，而當普通理論不明白時，須常常求助於特例。

14. 問題　求任何一數目m之一切因子之和。

〔解法〕 設 $m=p^a q^b r^c \cdots v^l$，於此 $p,q,r\cdots v$ 爲不同的質數，$a,b,c\cdots l$ 爲正整數。設m之一切因子，一與m自身亦包在內，爲 $d_1,d_2,d_3,\cdots d_k$，而設 $d_1+d_2+\cdots+d_k=S(m)$。

m 之每一因子，其形式爲 $d=p^{a'}q^{b'}r^{c'}\cdots v^{l'}$，於此 $a',b',c'\cdots l'$ 可爲任何以下値之結合：

$a'=0,1,2\cdots a$； $b'=0,1,2,\cdots b$； $\cdots l'=0,1,2\cdots l$。

反之，凡此形式的式乃是因子。

又，每一此形式的式遇見一次，亦祇遇見一次，爲以下之積之項，而此積無有他項：

$P=(1+p+p^2+\cdots+p^a)(1+q+q^2+\cdots+q^a)\cdots(1+v+v^2+\cdots+v^l)$。故$P$乃是諸 d 之和；但P之每一因子是一幾何級數，因得：

$$S(m)=\frac{p^{a+1}-1}{p-1}\cdot\frac{q^{b+1}-1}{q-1}\cdots\frac{v^{l+1}-1}{v-1}。$$

例 (1) 因 $25=5^2$，$S(25)=\dfrac{5^3-1}{5-1}=31$。

(2) 因 $72=2^3\cdot3^2$，$S(72)=\dfrac{2^4-1}{2-1}\cdot\dfrac{3^3-1}{3-1}$

$=15\cdot13=195$。

(3) 因 $100,800=2^6\cdot3^2\cdot5^2\cdot7$，$S(100,800)$

$$=\frac{2^7-1}{2-1}\cdot\frac{3^3-1}{3-1}\cdot\frac{5^3-1}{5-1}\cdot\frac{7^2-1}{7-1}=127\cdot13\cdot31\cdot8=409,448。$$

15．定義　一數目等於其一切因子(除自身)之和者，爲“完數。”例如 6 與 28 是完數，因 $6=3+2+1$，$28=14+7+4+2+1$。

16．定理　設 2^k-1 爲質數，則 $2^{k-1}(2^k-1)$ 爲完數。(此定理爲歐几里得所得)

〔證〕　設 $n=2^{k-1}(2^k-1)$，而設 $p=2^k-1$，則 $n=2^{k-1}p$。由 14 節，知 $S(n)=\frac{2^{(k-1)+1}-1}{2-1}\cdot\frac{p^2-1}{p-1}=(2^k-1)(p+1)=(2^k-1)2^k$。

於兩端減去 n，得

$$S(n)-n=(2^k-1)2^k-2^{k-1}(2^k-1)=(2^k-1)(2^k-2^{k-1})=(2^k-1)(2\cdot2^{k-1}-2^{k-1})=(2^k-1)2^{k-1}=n。$$

即是，n 是一完數。

17．我們不難證明，每一偶完數，其形式如前

者。至今尚未發見奇完數，亦不知有無此項存在。

18. 現在自然引起此問題，k 之何值能使 2^k-1 爲質數。第一條件自然 k 本身須爲質數，蓋若 $k=ab$，則照初等代數學 $2^{ab}-1$ 可有因子 2^a-1。1644年時，墨人耐(*Mersenne*)曾斷定若 p 爲一質數不大於257，則祗當

$$p=2,3,5,7,13,17,19,31,61,127,257,$$

時，2^p-1 是一質數。此形式的數目，2^p-1，$p \leqq 257$，名"墨氏數"。此中 p 之前九個值，均已證明，將其代入歐氏式中卽得九個完數。事實上，前八個十六世紀時已知之，第九個則十九世紀時纔證明。還有二個 $p=127$，257，則至今尚在可疑中。而當 $p<257$ 之值爲以前所列諸值以外者，2^p-1 卽非質數，於許多例亦均已證明，惟尚未全部證得。或者墨氏對於此問題另有其他有力的普通方法研究之，而其後人則未重發見此。

III. 地哇范土司(Diophantus)之方程

19. 定義 一方程中有二個或多於二個未知數，其值須為整數者，名為"地哇范土司方程;"亦稱"無定方程。"

一次的地氏方程，最好於本論之他部分中論之(31-33節)。

20. 二次的地氏方程之一可注意的例，乃是

$$x^2+y^2=z^2 \qquad (1)$$

任何一組滿足此方程的數目，是一直角三角形之三邊。故求前方程之一切整數的解，與求一切整邊的直角三角形，此二問題相同。如此的三角形，名"皮太谷人三角形"(*Pythagorean triangles*)。而若所得的解中 x,y,z 無公因子，則名為"質解"。事實上，我們祇要求得一切質解便够，蓋任何非質解均可用相當的因子乘其各數自一質解得之。

在入手求質解時，可先證明，於一質解之二數目 x 與 y 中，必一個是奇而其他則為偶。蓋設 (*a*) x 與 y 均為偶，則 z 亦必為偶；於是可有公因子 2，而非質解了。(*b*) 若 x 與 y 均為奇（即是，作

$2n+1$ 形式者)，x^2 與 y^2 即均作 $4n+1$ 形式，而 z^2 則作 $4n+2$ 形式。但這是不可能的，因每偶數之平方，其形式爲 $4n$，而每奇數之平方則作 $4n+1$。(a)與(b)既均不對，故 x 與 y 必是一偶一奇。今設 x 爲偶者，則 y 與 z 均爲奇。

由(1)： $$x^2=z^2-y^2=(z+y)(z-y)。$$

因 z 與 y 均爲奇，可設 $z+y=2k$，$z-y=2l$ (2)

故 $$x^2=4kl。$$

又因 x,y,z 爲互質的，k 與 l 亦必如此；蓋由 (2) $z=k+l$，$y=k-l$，故若 k 與 l 有公因子，y 與 z 亦必有此了。

因 $4kl$ 是一平方，故知 k 與 l 必爲方的。今可設：

$$k=m^2,\quad l=q^2\ (m,\ q\text{互質的})。$$

故(1)之任何質解內，x,y,z 必作此形式：

$$\left.\begin{aligned} x&=2mq\\ y&=m^2-q^2\\ z&=m^2+q^2\end{aligned}\right\}\qquad(3)$$

我們不難明白，每一組作此形式的值，不問其爲質數與否，能滿足此方程，我們可用下法自這些形式的解中選出其質者:

設m與q有公因子，則x,y,z亦必有此。故質解在限制m與q爲互質者之中。

又，因$z+y=2m^2$，$z-y=2q^2$，故z與y之任何公因子，乃是$2m^2$及$2q^2$之公因子，或，設m與q爲互質，是2之公因子。此即是，設m與q爲互質，則z與y至多祗能有2爲公因子。若m與q均爲奇，卽能有此，不則無（m與q爲互質）。如是，已證得。

定理 $x^2+y^2=z^2$之一切質解，沒有其他者，爲(3)所定出，祇須m與q取一切可能的互質值之組，$m>q$，而一奇一偶。

若有此，則祇要用數代入以作出一較小的質解之表。

定理 x,y,z三數中，一可用3除一（或卽前者）可用4除，其一則可用5除。

〔證〕 因m與q中有一爲偶者，x可用4除。設m或q可用3或5除，x卽可用3或5除。設m與q均不能用3除，則必均作$3n\pm1$形式，其平方之形式爲$3n+1$。故m^2-q^2作$3n$形式。此卽是y爲3之倍數。又設m與q均不能用5除，則其形式必作$5n\pm1$或$5n\pm2$，而其平方之形式爲$5n\pm1$。倘m^2與q^2同形式($5n+1$或$5n-1$)，m^2-q^2卽作$5n$形式；而倘一作$5n+1$，一作$5n-1$形式，m^2+q^2卽作$5n$形式。如爲前者，y爲5之倍數；爲後者則z爲5之倍數。(讀者於此倘感困難可找例證之)

21. 解$x^2+y^2=z^2$旣如是其易，於是自然想求$z^3=x^3+y^3$之解，然此則失望了。歐拉(*Euler*)曾證明，此方程不能解；卽是，沒有一整數之立方爲二整數之立方之和。而梵馬(*Fermat*)曾說過一普通廣定理如下：

倘n爲一正整數大於2，則$x^n+y^n=z^n$無整數的解。

此著名定理尋常名爲"梵馬之最後定理，"十七

世紀時梵氏說過但未附以證。自此以來，大費了許多算術家心力，欲求證明之而不能。雖對於許多特例已得其證，$n \leqq 100$ 時及其他有許多例均已證得，惟普通的證至今未得。

22. 還有一可注意的無定方程，亦極著名者如下：

$$x^2 - Dy^2 = \pm 1,$$

此方程通常稱為丕勒(*Pell*)氏方程，惟近來知道與丕氏實無關。但這裏不能詳論此方程。六世紀時，印度人已得解此方程之法，及至十八世紀時，拉格倫(*Lagrange*)獨自又得解法。此外還有許多其他無定方程，這裏均不能及。

IV. 相　合

23. 往往在有的問題中，諸數目，其差為一已知數之倍數者，是等值的。例如 (1) 以三角函數而論，凡角之差為 360° 之倍數者，此諸角是等值的；(2) 以(−1)一數目而論，其諸乘方之指數

倘以2之倍數相差，則其值是等的。

24. 定義 設$a=b+cm$，卽，設$a-b$爲m之倍數，則說：對於"率"(*modulus*)m而言，a與b"相合，"而寫作：

$$a\equiv b(mod.\ m) \qquad (1)$$

率總是假定其爲正的。如 (1) 那樣的關係，名爲一"相合式。"a與b對於率m相爲"餘"(*residues*)。符號$\equiv$兩旁之數，名爲相合式之"端。"下面數例，當不難明白其無誤：

$$15\equiv 8(mod.\ 7) \qquad 60\equiv 0(mod.\ 12)$$

$$37\equiv 19(mod.\ 6) \qquad -18\equiv 32(mod.\ 10)$$

$$1\equiv 41(mod.\ 5) \qquad 3\equiv -59(mod.\ 31)$$

25. 每一數目於以下一級數目中與一并祗與其一相合$(mod.\ m)$：

$$0,1,2,\cdots m-1;$$

於此級數目中亦然：$0,-1,-2,\cdots-(m-1)$；而設m爲奇，於此級中亦然：$0,\pm1,\pm2,\cdots\pm\frac{m-1}{2}$；

設m爲偶，即於此級中如此：$0, \pm 1, \pm 2, \cdots \pm \frac{m}{2} - 1, \pm \frac{m}{2}$。

這些名爲"至小正餘級，" "至小負餘級，"及"絕對至小餘級"$(mod.\ m)$。

26. 於任何相合式中，率之倍數可任意加上或減去之，於相合式無妨。蓋$a \equiv b\ (mod.\ m)$意義是a與b之差爲m之倍數，故設a或b或二者有m之倍數的變動，此屬性不受影響。即，設$ab \equiv c\ (mod.\ m)$，則$(a+dm)b \equiv c\ (mod.\ m)$。

讀者可自己試爲詳思。

27. 如是，任何相合式中之數目字的項及係數可約之使小於率，不致影響及於式。例如$83c \equiv 7\ (mod.\ 11)$可改之爲$9c \equiv 7\ (mod.\ 11)$，$437a + 289b \equiv 469c\ (mod.\ 27)$可改爲$5a + 19b \equiv 8c\ (mod.\ 27)$。(於此讀者可自己找些例練習)

28. 相合式之根本屬性。

I. 設$b \equiv a\ (mod.\ m)$而$c \equiv a\ (mod.\ m)$則$b \equiv c\ (mod.\ m)$。

〔證〕所設二相合式卽是$b=a+dm$，$c=a+em$。相減得$b-c=(d-e)m$。故$b\equiv c \pmod{m}$。

II. 設$a_1\equiv b_1 \pmod{m}$，$a_2\equiv b_2 \pmod{m}\cdots$ $a_l\equiv b_l \pmod{m}$，

則 $$a_1+a_2+\cdots+a_l\equiv b_1+b_2+\cdots+b_l \pmod{m}。$$

讀者可試自證之。又，以後其他處有不設證者，讀者均可自證之。

系　一相合式兩端之項可自一端遷至他端；卽可改其號而自一端遷至他端。

蓋設t為所欲遷的項，此卽無異於將$-t\equiv-t \pmod{m}$加於已知的式上。

III. 設　$a\equiv b \pmod{m}$，

則　$ka\equiv kb \pmod{m}$　幷$ka\equiv kb \pmod{km}$。

IV. 設$a\equiv b \pmod{m}$，而$c\equiv d \pmod{m}$，則$ac\equiv bd \pmod{m}$。

蓋由 *III* $ac\equiv bc \pmod{m}$ 而$bc\equiv bd \pmod{m}$ 故由 *I*. 卽得

$$ac\equiv bd \pmod{m}。$$

系1. 設 $a_1 \equiv b_1 (mod.\ m)$, $a_2 \equiv b_2 (mod.\ m)$, $\cdots a_l \equiv b_l (mod.\ m)$,

則 $$a_1 a_2 \cdots a_l \equiv b_1 b_2 \cdots b_l (mod.\ m)。$$

系2. 設$a \equiv b (mod.\ m)$，則 $a^r \equiv b^r (mod.\ m)$。

V. 設$a \equiv b (mod.\ m_1)$，$a \equiv b (mod.\ m_2) \cdots a \equiv b (mod.\ m_l)$，而設$M \equiv m_1, m_2, \cdots m_l$之最小公倍數，則$a \equiv b (mod.\ M)$。

〔證〕 照所設 $a-b=r_1 m_1, a-b=r_2 m_2, \cdots a-b =r_l m_l$，因 $a-b$ 爲$m_1, m_2 \cdots m_l$ 之倍數，故亦爲其最小公倍數之倍數。

29. 以前種種屬性，頗與代數方程方面之相當的諸屬性相類；不過這裏是"相合"非"相等"而已。這些屬性與加，減及乘相關。今將論乘之反，即因子分解，而看出，於此，方程之屬性與相合式之屬性間，其相類不如是之密切。

於方程方面，我們知道設$ab=0$，則$a=0$或$b=0$。但如$4 \cdot 6 \equiv 0 (mod.\ 12)$，則不必$4 \equiv 0 (mod.\ 12)$或$6 \equiv 0 (mod.\ 12)$。此即是，不能由$ab \equiv 0 (mod.$

m)推得$a\equiv 0$($mod.$ m)或$b\equiv 0$($mod.$ m)。

廣之，設知道$ab=ac$，而$a\neq 0$，則$b=c$。但設$ab\equiv ac$($mod.$ m)而$a\not\equiv 0$ ($mod.$ m)，則不必卽$b\equiv c$ ($mod.$ m)。

例如$2\cdot 21\equiv 2\cdot 17$($mod.$ 8)而$2\not\equiv 0$($mod.$ 8)，但不能$21\equiv 17$($mod.$ 8)。然於此有一屬性如下：

VI. 由$ab\equiv ac$($mod.$ m)，而a與m有最高公因子d，則可得

$$b\equiv c\left(mod.\ \frac{m}{d}\right)。$$

〔證〕 所設式卽是$ab=ac+km$，或$a(b-c)=km$。因m爲式左端之因子，d爲m之最大因子，並是a之因子，故$\frac{m}{d}$乃是$b-c$之因子，卽

$$b-c=k'\frac{m}{d}，或\ b\equiv c\left(mod.\ \frac{m}{d}\right)。$$

系 任何一相合式之二端可用一與率互質的因子除之，但若除數與率有公因子，則該因子亦必自率中取出。

例如 (1) $30\equiv 78$ ($mod.$ 12)，故可得 $5\equiv 13$

$(mod.\ 2)$。

(2) $108 \equiv 192\ (mod.\ 14)$，故得 $9 \equiv 16\ (mod.\ 7)$。

(3) $224 \equiv 44\ (mod.\ 15)$，故 $56 \equiv 11\ (mod.\ 15)$。

30. 相合觀念之應用　此種相合觀念及適纔所舉諸簡易屬性，已足解決許多有味的問題，今舉數例如下：

I. 大數目爲一已知的數目除時，試求其餘數。

(1) 設2^{40}爲23所除，可求其餘數：

我們知道 $2^5=32$，故$2^5 \equiv 9\ (mod.\ 23)$。方之得

$$2^{10} \equiv 81\ (mod.\ 23) \equiv 12\ (mod.\ 23),$$

再方之，$$2^{20} \equiv 144\ (mod.\ 23) \equiv 6\ (mod.\ 23),$$

再方之，$$2^{40} \equiv 36\ (mod.\ 23) \equiv 13\ (mod.\ 23)。$$

此卽2^{40}爲23除時餘數爲13。

(2) 試證明$2^{2^5}+1$有因子641（見10節）：

欲證明此祗須證出2^{2^5}或2^{32}爲641所除時，有餘數-1：

$2^2=4$，$2^4=16$，$2^8=256$，$2^{16}=65,536$
$\equiv 154 (mod. 641)$。

$2^{32}\equiv(154)^2 (mod. 641)\equiv 23,716 (mod. 641)$
$\equiv -1 (mod. 641)$。

這些問題內若取正或負的絕對至小餘，則可省乘的工作。

(3) 以下諸墨氏數目（見18節）及其因子用此法亦不難證明：

$2^{11}-1$之因子23。　　$2^{23}-1$之因子47。

$2^{29}-1$之因子233。　　$2^{37}-1$之因子223。

$2^{239}-1$之因子479。　　$2^{251}-1$之因子503。

(4) 若多費些計算工夫，可正確證明$2^{97}-1$之因子爲11,447，$2^{223}-1$之因子爲18,287，$2^{2^{12}}+1$之因子爲114,689，即10節中所說之$2^{2^{36}}+1$亦可用計算證實之，雖使人厭倦，然此方法之有效，則於此可見一極注意的例。

如前之因子，證明之固不難，然欲求得之則大不易。

II. 可除性之標準。

設如自右至左讀之,一數目N之各位數目字(十數以下者) 爲 $a,b,c,d,e,f,g,\cdots$,則得

$$N=a+10b+10^2c+10^3d+10^4e+10^5f+10^6g+\cdots$$

(1) 因$10\equiv1(mod.\ 9)$, 故照28節*IV*之系2,$10^2\equiv1(mod.\ 9)$, $10^3\equiv1(mod.\ 9)$,$\cdots$,我們可寫:

$$N\equiv a+b+c+d+\cdots(mod.\ 9)。$$

設$a+b+\cdots$是9之倍數, 則N卽爲9之倍數。此卽是有名的標準: 一數目當其各位數目字之和爲 9 之倍數時, 且祇當此時, 爲 9 之倍數。

(2) 因$10\equiv-1(mod.\ 11)$,故$10^2\equiv1(mod.\ 11)$, $10^3\equiv-1(mod.\ 11)$, $10^4\equiv1(mod.\ 11)$, $\cdots$, 我們可寫:

$$N\equiv a-b+c-d+e-f+\cdots(mod.\ 11)。$$

此卽是: 一數目當其奇位數目字之和減去其偶位數目字之和之差爲11之倍數時,且祇當此時,此數目是11之倍數。

(3) 因 $10^3+1=7\cdot11\cdot13$, 我們可求 7, 11, 或

13之可除性標準。於此，$10^3 \equiv -1 \ (mod.\ 10^3+1)$，故照28節*III*得以下諸相合式：

$$\left.\begin{aligned} &10^4 \equiv -10 \\ &10^5 \equiv -10^2 \\ &10^6 \equiv -10^3 \equiv -(-1) \equiv 1 \\ &10^7 \equiv 10 \\ &10^8 \equiv 10^2 \quad \text{等等} \end{aligned}\right\} (mod.\ 10^3+1)$$

故 $N \equiv (a+10+10^2c)-(d+10e+10^2f)+(g+10h+10^2j)-\cdots \ (mod.\ 10^3+1)$。於是可得以下7，11，13之可除性標準：

自右面起，將已知數目每三位作爲一段（左面末段自可少於三位）。將這些段看作爲位數目，往復變其號加之，設所得的代數和可爲7，11或13所除，則原數目卽可被此數除，否則不能。

例如847,963,207一數，欲探其能否爲7，11或13所除，可作

$$207-963+847=91。$$

因91可用7與13除，但不能用11除，故847,963,

207可爲7與13除，但11則不能除之。

一檢前面的證，可見設如此除數非爲一數目之因子，則除後餘數亦可由此得之。蓋可除性祇是其餘等於零而已。例如用9除一數之餘，與除其各位數之和之餘等。仿此，847,963,207一數用11除後得餘數3，而91爲11除時其餘數亦爲3。

31. 相合式之根　一相合式

$a_0x^n+a_1x^{n-1}+a_2x^{n-2}+\cdots+a_{n-2}x^2+a_{n-1}x+a_n\equiv 0$ $(mod.\ m)$，於此a爲任何數目，惟a_0非爲m之倍數，名爲x未知數之n次者。

任何一數目x_1代於x處時使左端與右端相合$(mod.\ m)$者，名爲能滿足此相合式，而爲此式之根。

設任何一數目x_1是一根，一切數目凡與x_1相合$(mod.\ m)$者亦滿足此相合式(26節)。然這些不能視爲不同的諸根。以m爲率，凡一切與x_1相合的數目視爲一值，任何其中之一可選以代表之；例如可選其最小正餘$(mod.\ m)$爲之。如是，0,1,2,

3,…$m-1$，諸數目代表一切存在的值$(mod.\ m)$；倘試其相合，無其他可能性。

用些特例，很易證明方程方面所有關於根之存在及數目的屬性，於相合式不能無改變應用。例如 $ax=b$ 方程總有一，亦祇有一根。但很易明白，相合式$ax\equiv b(mod.\ m)$則可以：

(1) 沒有根。 例如 $3x\equiv 5(mod.\ 9)$，任使 x 取以下一可能的值

$$x\equiv 0,1,2,3,4,5,6,7,8(mod.\ 9),$$

沒有能滿足相合式者。其實將前式寫作$3x-5\equiv 0$ $(mod.\ 9)$便已可見，蓋此即是須這樣選擇 x，俾 $3x-5$ 能爲9之倍數，然 x 無論如何，$3x-5$ 尙不能爲3之倍數，更不論爲9之倍數了。

(2) 有一根。 例如$5x\equiv 3(mod.\ 9)$，用九個 x 之可能的值試之，可知祇有 6 能滿足此，外此無其他。

(3) 多於一根。 例如$6x\equiv 3(mod.\ 9)$，試驗時可知2,5,8三值能滿足此式，此外即沒有了。

關於此下節還將詳論。以下的定理當不難證明之，此定理與代數學上之根本定理 n 次方程恰有 n 個根者相仿(參觀第五篇 7,10 二節，及第四篇附錄二)：

定理　n 次率爲質數的相合式，其根不能多於 n 個。

其證這裏不錄。讀者可仿方程方面之證法證之(第五篇10節)。

32. 一次一未知數的相合式之理論的解法

設有

$$ax\equiv b(mod.\ m),$$

(我們可假定 b 是正的小於 m。倘所設不如是則可加或減 m 之倍數使其如此)則可分數例論之：

例 *I.* a 對於 m 爲質的。於此，我們可於 ax 內 x 處更換代入 $0,1,2,\cdots m-1$，得 $ax=0,a,2a,3a,\cdots(m-1)a$。或取至小正餘 $(mod.\ m)$ $ax\equiv c_0(=0)$，c_1，c_2，$c_3\cdots c_{m-1}(mod.\ m)$。

能否 c 中有相等者？今假定 $c_k=c_h$ $k>h$。因照

定義$ka=c_k+rm$而$ha=c_h+sm$，故設$c_k=c_h$，即得

$$(k-h)a=(r-s)m。$$

但a對於m是質的，故$k-h$爲m之倍數。惟$k-h$是正的，而k小於m，乃是$1,2,\cdots m-1$中之一數，故$k-h$小於m，不能爲m之倍數。因此，設$c_k=c_h$不合理，而諸c均不同的。因其數有m個，每個是m個數目$0,1,2,\cdots m-1$中之一，而又各各不同，故知諸c必即爲$0,1,2,\cdots m-1$諸數目作任何一種次序。

於此末組數目中，b遇見一次，亦祇一次。故必恰有一c等於b，或恰有x之一值能$ax\equiv b(mod.\ m)$者。於是知：

一次相合式中未知數之係數對於其率爲質者有一解且祇有一解。

例II. 設a與m有最高公因子$d>1$。

相合式$ax\equiv b(mod.\ m)$意即是$ax=b+km$。因a與m有因子d，故此方程中之b亦必有此，不則不合理。此即是，設$b\not\equiv 0(mod.\ d)$此相合式不

能解。今設$b\equiv 0 \pmod{d}$，而設$a=a_1d$，$b=b_1d$，$m=m_1d$（a_1 對 m_1 爲質，因d爲a與m之最高公因子）。則可用d將相合式幷率除之，得

$$a_1x\equiv b_1 \pmod{m_1}。$$

照 28 節 *III*，此式之每一根卽是所設式之根。但此式卽爲前例，有一根且祇有一根。今設此根爲r，則一切作$r+km_1$形式的數目對於率m_1均是等值的，故均能滿足此式。但是否對於其率m這些是與一單獨的解等值的？

今設$r+k_1m_1$與$r+k_2m_1$（$k_1>k_2$）照率m是等值的。卽$r+k_1m_1\equiv r+k_2m_1 \pmod{m}$或$(k_1-k_2)m_1\equiv 0 \pmod{m}$。故用$m_1$除式之兩端幷率，得

$$k_1-k_2\equiv 0 \pmod{d}\text{或}k_1\equiv k_2 \pmod{d}。$$

此卽是，$r+km_1$形式的二數目，祇當k相合（mod. d.）時，纔相合（mod. m）。故所設的相合式有d個解，由$r+km_1$內將k依次給以$0,1,2,3,\cdots d-1$等諸數得之。

例：(1) $12x\equiv 6 \pmod{15}$。於此$d=3$，$m_1=5$。

用d除，得$4x\equiv2(mod.5)$。由試驗，可見此式能爲 $x\equiv3\ (mod.\ 5)$ 所滿足。這裏$r=3$，$r+km$ 爲 $3+5k$。依次給 k 以 0,1,2，卽得 3,8,13 爲根 $(mod.\ 15)$。

(2) $8x\equiv12(mod.\ 28)$。於此 $d=4$，$m_1=7$。用 4 除得 $2x\equiv3(mod.\ 7)$。由試驗，可見其爲 $x\equiv5\ (mod.\ 7)$ 所滿足。這裏 $r=5$，$r+km$ 爲 $5+7k$。使k取 0,1,2,3，卽得四根 5,12,19,26 $(mod.\ 28)$。

33. ax≡b(mod. m)之數字的解法 前面的研究祇證明某例內有一根或多根之存在，但除了試驗以外無法求其數字的值。倘能求得一種方法對於a與m爲互質時可用卽已够，蓋如前所見，相合式中a與m非爲互質時，其解亦可由解—a與m爲互質的式得之。

此外，更確定此事實，卽 $ax\equiv b(mod.\ m)$之解，可由 $ax\equiv1(mod.\ m)$之解得之。蓋設 r 爲後者之根，則$ar\equiv1(mod.m)$，而用b乘時，得$a(br)\equiv b\ (mod.\ m)$。此卽是 br 爲原式之解。故此問題在

於求$ax\equiv1(mod.\ m)$之解。但在此式內實有二未知數，x以及率之倍數y。卽是，須求x與y之值，能滿足$ax=1+my$或$ax-my=1$者。然後者之方程爲連分理論上所熟知者。設如分數$\frac{a}{m}$化爲一連分，而設$\frac{Y}{X}$爲到$\frac{a}{m}$值前之末近數，則我們知道可有此關係$aX-mY=\pm1$。故X或$-X$爲$ax\equiv1(mod.\ m)$之根。

於是得下面計算$ax\equiv b(mod.\ m)$之根之規法：將$\frac{a}{m}$化成連分。淬到$\frac{a}{m}$以前之末近數之分母乃是$ax\equiv1(mod.\ m)$之根之絕對值。其號可用試驗決定之；而如是所得值用b乘之卽爲$ax\equiv b(mod.\ m)$之根。

〔附註〕凡作如是形式的式：

$$a+\cfrac{1}{b+\cfrac{1}{c+\cfrac{1}{d+\cdots}}}$$

〔a爲一整數，$b,c,d,\cdots$爲正整數〕

名爲連分。每有理分數可作爲一有盡連分表之，例如

$$-\frac{29}{11}=-3+\frac{4}{11}=-3+\frac{1}{\frac{11}{4}}=-3+\frac{1}{2+\frac{3}{4}}=$$

$$-3+\frac{1}{2+\frac{1}{\frac{4}{3}}}=-3+\frac{1}{2+\frac{1}{1+\frac{1}{3}}}。$$

$\frac{a}{1}$，$a+\frac{1}{b}$，$a+\frac{1}{b+\frac{1}{c}}$等等名爲其第一，第二，第三，等等近數。如前例之近數爲-3，$-3+\frac{1}{2}$，$-3+\frac{1}{2+\frac{1}{1}}$，$-3+\frac{1}{2+\frac{1}{1+\frac{1}{3}}}$，或約作$-3$，$-\frac{5}{2}$等等。

例如：$49x\equiv 23(mod.\ 125)$。

$$\frac{49}{125}=\frac{1}{2+\frac{1}{1+\frac{1}{1+\frac{1}{4+\frac{1}{2+\frac{1}{2}}}}}}$$

其末近數爲$\frac{20}{51}$。故$X=51$。由試驗，得

$$49 \cdot 51 \equiv -1 \pmod{125},$$

此卽是，-51 乃是 $49x \equiv 1 \pmod{125}$ 之解。用 23 乘 -51，卽得原式之解：

$$23(-51) \equiv 77 \pmod{125}。$$

試將 77 代入，卽可證明其爲原式之解。(讀者可找些例[illegible])

34. 梵馬之定理　設 p 爲質數，a 對 p 爲質的，則 $a^{p-1} \equiv 1 \pmod{p}$。此定理1679年時梵氏所述，未附以證。1736年時歐拉始證明之。但於 $a=2$，則中國人在二千四百年以前已知此定理了。

〔證〕32節中已證明，$a, 2a, 3a, \cdots (p-1)a$ 諸數與 $1, 2, 3, \cdots p-1$ 諸餘相合 $\pmod{p}$〔祇須記得 $0 \equiv 0 \pmod{p}$，則由32節之結果卽得此〕。將這些相合式乘之，得

$$a \cdot 2a \cdot 3a \cdots (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdots p-1 \pmod{p}。$$

用 $1 \cdot 2 \cdot 3 \cdots p-1$ (此對於率爲質者)除其兩端，卽得所求者：

$$a^{p-1} \equiv 1 \pmod{p}$$

35. **應用** (1)試求一次數小於13的相合式，與以下式等值者：

$$x^{27}+3x^{25}+4x^{18}-3x^{17}+6x^{13}-2x^{7}+11x-5$$
$$\equiv 0\ (mod.\ 13)$$

由視察，可知 $x\equiv 0\ (mod.\ 13)$ 不能滿足此式；故知任何一根 x 對13是質的，而 $x^{13-1}\equiv 1\ (mod.\ 13)$。又，

$$x^{27}=(x^{12})^{2}\cdot x^{3}\equiv(1)^{2}x^{3}\equiv x^{3}\ (mod. 13),$$

$$3x^{25}=3(x^{12})^{2}\cdot x\equiv 3x\ (mod.\ 13),\ 4x^{18}=4x^{12}\cdot x^{6}$$
$$\equiv 4x^{6}\ (mod.\ 13),$$

$$3x^{17}\equiv 3x^{5}\ (mod.\ 13),\quad 6x^{13}\equiv 6x\ (mod.\ 13)。$$

將這些代入原式，得

$$-2x^{7}+4x^{6}-3x^{5}+x^{3}+20x-5\equiv 0\ (mod.\ 13)。$$

(2) 試求47^{7385}被17除後之餘。

用$17-1$即16除7385，得$7385=461\cdot 16+9$。故

$$47^{7385}=(47^{16})^{461}\cdot 47^{9}\equiv(1)^{461}\cdot 47^{9}\ (mod.\ 17)。$$

但 $47=2\cdot 17+13$或$47\equiv 13\ (mod.\ 17)$，故照28節IV系2，

$(47)^9 \equiv 13^9 (mod.\ 17)$，或 $47^{7385} \equiv 13^9 (mod.\ 17)$。

今再求 13^9：$13^2 = 169 \equiv -1 (mod.\ 17)$；方之，得 $13^4 \equiv 1 (mod.\ 17)$；再方之，$13^8 \equiv 1 (mod.\ 17)$。用13乘其兩端，得 $13^9 \equiv 13 (mod.\ 17)$，故

$$47^{7385} \equiv 13 (mod.\ 17)。$$

而13即是餘。(讀者可隨找幾個例自己練習)

(3) 設 $n>1$ 爲一整數，試證明 $n^{13}-n$ 有因子2730。

因 $2730 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 13$，故祇須證明 $n^{13}-n$ 有此諸因子便得。今先證因子2。$n^{13}-n = n(n^{12}-1)$。設 n 爲偶數，則自然即有2爲因子。設 n 爲奇數，則可證明 $n^{12}-1$ 是偶的。實際上，此是極明白者，蓋奇數之乘方總是奇的，n^{12} 是奇，而 $n^{12}-1$ 則爲偶。

由梵氏定理，還可知，因 n 對於2爲質：$n^{2-1} \equiv 1 (mod.\ 2)$。

故　　$n^{12} = (n^{2-1})^{12} \equiv 1 (mod.\ 2)$ 或 $n^{12}-1 \equiv 0$

$(mod. 2)$。

再證因子 3。如前，n 若非為 3 之倍數，必證明 $n^{12}-1$ 為 3 之倍數纔行。照梵氏定理 $n^{3-1}\equiv 1$ $(mod. 3)$。故

$$n^{12}=(n^{3-1})^6\equiv 1 (mod. 3) \text{而} n^{12}-1\equiv 0 (mod. 3)。$$

用此法并可證明5,7,13為因子，而所求者證明了。

(4) 試證明每一質數 (2與5除外) 乃是其一切位均為9的數目之因子。

設p為2與5以外之質數。則 10^n 對於p為質的。故照梵氏定理 $(10^n)^{p-1}-1\equiv 0$ $(mod. p)$。此則於每個n均合理。而$(10^n)^{p-1}-1$總是祇為 9 所成的數目，故所說者已證明。

(5) $ax\equiv b (mod. p)$ (a對於p為質的)，可用a^{p-2}乘其兩端而應用梵氏定理解之，得結果$x\equiv ba^{p-2}$ $(mod. p)$。

36. 惠爾遜定理 (Wilson's Theorem) 設p

為質數，則$(p-1)!\equiv -1 \pmod{p}$。

設$p=2$，此定理卽自明的，故可假定$p>2$而證之；但須先證此

補題　$ax\equiv 1 \pmod{p}$之根，倘$a\equiv 1$或$a\equiv p-1 \pmod{p}$，且祇是如此，乃與a相合。

〔證〕由32節，$ax\equiv 1 \pmod{p}$有一根。今假定其為a，則

$$a^2\equiv 1 \pmod{p} \text{或} (a-1)(a+1)\equiv 0 \pmod{p}。$$

但祇當一因子為一質數p之倍數時，一乘積纔能為一質數p之倍數，故必$a-1\equiv 0$或$a+1\equiv 0 \pmod{p}$。此卽是補題所說者。

今設a_1為$2,3,\cdots p-2$中之一數目，則照補題，$a_1x\equiv 1 \pmod{p}$之根將與a_1異；今命之為a_2，則得$a_1a_2\equiv 1 \pmod{p}$。試再論前者中之第三數目a_3，而用a_4表$a_3x\equiv 1 \pmod{p}$之根，則得$a_3a_4\equiv 1 \pmod{p}$，照補題，a_4與a_3不相合。并可證明其與a_2亦不相合。蓋若$a_2\equiv a_4 \pmod{p}$，則用a_3乘兩端時，

$$a_3a_2 \equiv a_3a_4 \pmod{p} \text{或} a_3a_2 \equiv 1 \pmod{p}。$$

但我們知 $a_1a_2 \equiv 1 \pmod{p}$，故 $a_3a_2 \equiv a_1a_2 \pmod{p}$。用 a_2 除兩端時，可得 $a_3 \equiv a_1 \pmod{p}$。此則與所設 a_3 與 a_1 異矛盾。故知不能設 $a_2 \equiv a_4 \pmod{p}$。仿此可知 $a_4 \not\equiv a_1 \pmod{p}$。

今設 a_5 爲一第五數目與前所論者異，而設 a_6 爲 $a_5x \equiv 1 \pmod{p}$ 之根，則可知 a_6 不能與 $a_1, \cdots a_5$ 中任何一相合。如此下去，可將 $2, 3, \cdots p-2$ 諸數目盡成爲對，俾每對之積相合 $1 \pmod{p}$。

即是

$$\left.\begin{array}{r} a_1a_2 \equiv 1 \\ a_3a_4 \equiv 1 \\ \cdots\cdots\cdots \\ a_{p-4}a_{p-3} \equiv 1 \end{array}\right\} \pmod{p}。$$

此外，$p-1 \equiv -1 \pmod{p}$，故將此諸式乘之，并記牢諸 a 乃是 $2, 3, \cdots p-2$ 諸數，即得 $2 \cdot 3 \cdots (p-2)(p-1) \equiv -1 \pmod{p}$，或

$$(p-1)! \equiv -1 \pmod{p}。$$

37. 惠氏定理於複數率不能用。蓋設 m 爲複數，

k為其一因子$(1<k<m)$，則$(m-1)!$可有k為因子，故$(m-1)!+1$不能為k之倍數，卽不能為m之倍數。因此，惠氏定理於理論上實為決定一已知數是否為質數之完全標準。例如有一數n，欲探其是否為質，可作出$(n-1)!$，用n除之，設得餘數-1，n卽為質，否則非是。但此法於大數目，因計算功夫太大，實不能用。

38. 應用 (1)設p為質數，則當$(p-1)!$為$1+2+\cdots+(p-1)$所除時，其餘是$p-1$。卽是$(p-1)!\equiv p-1(mod.\ 1+2+\cdots+[p-1])$。

由惠氏定理，　　$(p-1)!=-1+kp=(k-1)p+(p-1)$。

因此式左端有因子$(p-1)$，而右端之第二項為$p-1$，故知$(k-1)p$必有因子$p-1$，而因$p-1$對於p為質的，卽$k-1$有因子$p-1$。

今設$k-1=h(p-1)$。代入，卽得

$$(p-1)!=h(p-1)p+p-1=2h\frac{(p-1)p}{2}+p-1.$$

但$\frac{(p-1)p}{2}=1+2+\cdots+(p-1)$，故所設者已證明。

(2) 設有一質數作$4n+1$形式，則$(1\cdot2\cdots2n)^2+1$爲p之倍數。

照惠氏定理$(p-1)!+1\equiv0\ (mod.\ p)$或$(4n)!+1\equiv0\ (mod.\ p)$ (1)

但因$p=4n+1$，

$$\left.\begin{array}{l} 4n\equiv-1 \\ 4n-1\equiv-2 \\ \cdots\cdots\cdots\cdots \\ 2n+2\equiv-(2n-1) \\ 2n+1\equiv-2n \end{array}\right\}(mod.\ p),$$

故 $(2n+1)(2n+2)\cdots(4n-1)(4n)\equiv(-1)^{2n}(2n)!\ (mod.\ p)$ (2)

由(2)與(1)，得 $(1\cdot2\cdot3\cdots2n)^2+1\equiv0\ (mod.\ p)$。

V. 二項相合式

39. 定義 作$x^n-A\equiv0\ (mod.\ m)$形式的相合

式，名爲"二項相合式"。

我們祇論$x^n-1\equiv 0(mod.\ p)$，於此p爲一質數。由梵氏定理，總可以使$n<p$。設$p=2$，此式卽爲一次的，前已解之。故於論二項相合式內，均假定p爲一質數大於2者。

40. $x^m\equiv 1(mod.\ p)$之諸解(m爲任何正整數)必對p爲質的，故照梵氏定理幷爲$x^{p-1}\equiv 1(mod.\ p)$之解。又照28節IV之系2，$x^m\equiv 1(mod.\ p)$之每一解，亦爲$x^{km}\equiv 1(mod.\ p)$之解。

41. 定理 設α爲$x^n\equiv 1(mod.\ p)$之根，幷爲$x^q\equiv 1(mod.\ p)$之根，而設d爲n與q之最高公因子，則α爲$x^d\equiv 1(mod.\ p)$之根。

〔證〕 設$n=n'd$，$q=q'd$。則n'與q'是互質的，而

$$n'z\equiv 1(mod.\ q')$$

有一解，卽是，可有數目z與y存在，滿足

$$n'z=1+yq'\text{或}n'z-yq'=1$$

者。用d乘之，得$nz-yq=d$。照所設$\alpha^n\equiv 1(mod.$

p)，故 $\alpha^{nz}\equiv 1\ (mod.\ p)$，而 $\alpha^{q}\equiv 1\ (mod.\ p)$，故 $\alpha^{qy}\equiv 1\ (mod.\ p)$。

相減，得 $\alpha^{nz}-\alpha^{qy}\equiv 0\ (mod.\ p)$ 或 $\alpha^{qy}\ (\alpha^{nz-qy}-1)\equiv 0\ (mod.\ p)$。

因α對p爲質，故　　$\alpha^{nz-qy}-1\equiv 0\ (mod.\ p)$

或　　$\alpha^{d}-1\equiv 0\ (mod.\ p)$。

卽是α爲$x^{d}\equiv 1\ (mod.\ p)$之根。

系　設 d 爲 n 與 $p-1$ 之最高公因子，則$x^{n}\equiv 1\ (mod.\ p)$之解，亦能滿足$x^{d}\equiv 1\ (mod.\ p)$。

因此，祇須論如是的相合式：

$$x^{d}\equiv 1\ (mod.\ p),\ (d\text{爲}p-1\text{之除數})。$$

42. 定義　設 $a^{d}\equiv 1\ (mod.\ p)$而$a^{y}\not\equiv 1\ (mod.\ p)$ $(y<d)$，則云a"屬於"指數$d\ (mod.\ p)$。

43. 定理　設a屬於指數 $d\ (mod.\ p)$，則當 t 爲 d 之倍數時，且祇當此時，$a^{t}\equiv 1\ (mod.\ p)$。

〔證〕設 $a^{t}\equiv 1\ (mod.\ p)$，而設D爲t與d之最高公因子，則照41節 $a^{D}\equiv 1\ (mod.\ p)$。倘 t 非爲d之倍數，$D<d$，如是 a 將能滿足一相合式小於d次

爲D次者了。故t必爲d之倍數。

44. 定理 設a屬於指數r，b屬於指數$s\ (mod.\ p)$，而設r與s互質，則ab屬於指數$rs\ (mod.\ p)$。

〔證〕所設者卽是$a^r\equiv1\ (mod.\ p)$，$b^s\equiv1\ (mod.\ p)$，而a與b不能滿足次數較低的式。今祇須證明(1) $(ab)^{rs}\equiv1\ (mod.\ p)$，以及(2)$ab$之較低的乘方不與$1\ (mod.\ p)$相合。

(1) $(ab)^{rs}=a^{rs}b^{rs}=(a^r)^s\cdot(b^s)^r\equiv1^s\cdot1^r\ (mod.\ p)$
$\equiv1\ (mod.\ p)$。

(2) 設k爲任何一指數，能$(ab)^k\equiv1\ (mod.\ p)$卽$a^k\cdot b^k\equiv1\ (mod.\ p)$者。將此兩端方至$r$次，得$a^{rk}\cdot b^{rk}\equiv1\ (mod.\ p)$。但因$a^r\equiv1\ (mod.\ p)$，故$b^{rk}\equiv1\ (mod.\ p)$。然$b$屬於$s$,故$rk$爲$s$之倍數,因$r$與$s$互質，$k$卽爲$s$之倍數。仿此，并可證明$k$爲$r$之倍數。$r$與$s$既互質，故$k$爲$rs$之倍數，其最低値爲$rs$本身，於是可知$ab$屬於$rs$。

45. 設r與s不互質，而設m爲其最小公倍數；則同樣的可證明有一屬於m的數目能爲a與b所

決定。

46. 定理 對於$p-1$之每一除數d至少有一數目a屬$(mod.\ p)$之。

〔證〕 (1)先設$d=q^a$(q爲質數)。則

$$x^{p-1}-1\equiv 0\ (mod.\ p) \qquad (1)$$

可寫作

$$x^{fq^a}-1\equiv 0\ (mod.\ p) \qquad (2)$$

或 $(x^{q^a}-1)\ (x^{(f-1)q^a}+x^{(f-2)q^a}+\cdots+x^{q^a}+1)\equiv 0$

$(mod.\ p)$。 (3)

由梵氏定理，(1)於x之每一值除$\equiv 0\ (mod.\ p)$者外均能滿足。故(3)有最大數的根。但(3)之左端之因子，沒有能與0相合時其根多於次數者，故每一因子與零相合之根與次數同多。詳之，

$$x^{q^a}-1\equiv 0\ (mod.\ p) \qquad (4)$$

有q^a根。有的亦能滿足此種式及較低次的式。照40與41節，這些根均滿足$x^{q^{a-1}}-1\equiv 0\ (mod.\ p)$。但如適纔所說，此式恰有$q^{a-1}$根，故恰有(4)之$q^a-q^{a-1}$或$q^{a-1}(q-1)$根不能滿足較低次的式者。此卽是，恰有$q^{a-1}(q-1)$不相合的數目屬於指數

q^{α}者。

(2) 又設d爲$p-1$之任何除數。則可使 $d=q^{\alpha}r^{\beta}s^{\gamma}\cdots$($q,r,s$ 爲不同的質數)，而照 (1)，可有一數目 a 屬於q^{α}，一數目 b屬於r^{β}。故由44節定理ab屬於 $q^{\alpha}r^{\beta}$。

由 (1) 可有一數目 c 屬於 s^{γ}。因 $q^{\alpha}r^{\beta}$與s^{γ}互質，abc 屬於 $q^{\alpha}r^{\beta}s^{\gamma}$。如此下去，盡及$d$之一切因子，於是卽得一屬於$d$的數目。

系 至少有一數目g屬於$p-1$者。

47. 定義 設g屬於指數$p-1$，則g稱爲

$$x^{p-1}\equiv 1 \pmod{p}$$

之"質根"，或簡稱p之質根。

48. 定理 設g爲p之質根，則$g,g^2,g^3,\cdots g^{p-1}$諸數是不同的$(mod.\ p)$而有餘數$1,2,3,\cdots p-1$作某種次序。

〔證〕設 $g^h\equiv g^k\ (mod.\ p)$，$p-1\geqq h>k\geqq 1$，則 $g^{h-k}\equiv 1\ (mod.\ p)$。但 $p-1>h-k\geqq 1$，故此與所設g爲p之質根相違。因之，$g,g^2,\cdots g^{p-1}$ 之餘不

同$(mod.\ p)$，而爲$1,2,\cdots p-1$作某種次序。

49. 定理　設g爲p之質根，而k對於$p-1$爲質的，則g^k爲p之質根。

〔證〕設$(g^k)^h\equiv1(mod.\ p)$。則因g屬於指數$p-1$，$kh\equiv0(mod.\ p-1)$。而k既對$p-1$爲質，故即$h\equiv0(mod.\ p-1)$。

h之最小值爲$p-1$；此即是g^k屬於指數$p-1$，故爲p之質根。

系　p有$\phi(p-1)$個質根。

50. 設率不大，則質根之實際值可用試驗得之。

例如$p=17$，可試以2：

$$\left.\begin{array}{ll} 2=2 & 2^5\equiv-2 \\ 2^2=4 & 2^6\equiv-4 \\ 2^2=8 & 2^7\equiv-8 \\ 2^4=16\equiv-1(mod.\ 17) & 2^8\equiv-16\equiv1 \end{array}\right\}(mod.\ 17)$$

此即是，2屬於指數8，非爲17之質根。即所得諸餘2,4,8,16,15$(\equiv-2)$,13,9,1,亦不能爲質根。蓋其形式均作2^k,而$(2^k)^8$或$2^{8k}\equiv1(mod.\ p)$，因2^8

是如此。故此一切餘或屬於8或屬於8之除數。

末在前者中之最小的數目，乃是3。試以3，可知其爲屬於指數16者；故3爲17之質根。

我們幷可不用試驗證明3必爲質根。蓋因$\phi(16)=8$，17有8個質根。但2^k有8餘，均非質根，故每一其他8個非爲零的餘必爲質根。而3是一質根。

倘第二試驗仍不能引至質根，則前面的定理(44與45節）能使我們決定一數目，屬於二指數之最小公倍數者。設此最小公倍數爲$p-1$本身，卽得一質根。如不然，則至少有一數屬於一更大的指數者，而其乘方自不必再論。如是，系統的試驗能使我們求得質根。

對於大的質數，自多費計算功夫。關於此曾得數條普通定理。

例如：設如一質數作 $2^{2^n}+1$ 形式，則有質根 3。

又：設如一質數作 $8n+3$ 形式，而設 $4n+1$ 亦質數，則此質數有質根2。

VI. 二次相合式

51. 最普通一未知數的二次相合式，是

$$ax^2+bx+c\equiv 0 \pmod{m}。$$

可簡其形式如下：用$4a$乘兩端及率，得

$$4a^2x^2+4abx+4ac\equiv 0 \pmod{4am},$$

或 $$(2ax+b)^2-b^2+4ac\equiv 0 \pmod{4am}。$$

設 $y\equiv 2ax+b \pmod{4am}$，$d\equiv b^2-4ac \pmod{4am}$，

則前式作 $$y^2\equiv d \pmod{4am}。$$

由y之值，可得x之值，祇須解以下之一次式便行：

$$y\equiv 2ax+b \pmod{4am}。$$

52. 設$4am=p_1^{k_1}\cdot p_2^{k_2}\cdots p_l^{k_l}$（$p_1, p_2, \cdots p_l$為不同的質數），則任何數目之滿足

$$y^2-d\equiv 0 \pmod{4am} \qquad (1)$$

者，亦能滿足以下各式：

$$\left.\begin{array}{l} y^2-d\equiv 0 \pmod{p_1^{k_1}} \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ y^2-d\equiv 0 \pmod{p_l^{k_l}} \end{array}\right\} \qquad (2)$$

反之亦然。

53. 於是解普通二次式之問題，化爲解此項的式：

$$x^2-a\equiv 0\ (mod.\ p^k)\quad (p\text{爲質數})。$$

此式之任何解，亦爲下式之解：

$$x^2-a\equiv 0\ (mod.\ p^h)\quad (h<k)。$$

及
$$x^2-a\equiv 0\ (mod.\ p)\qquad (3)$$

以後所論，將限於此式者；今取率 7 爲先例。試作七個至小正餘 $(mod.\ 7)$ 之方，得

$$0^2\equiv 0,\ 2^2\equiv 4,\ 4^2\equiv 2,\ 6^2\equiv 1,\ 1^2\equiv 1,\ 3^2\equiv 2,\ 5^2\equiv 4\ (mod.\ 7)。$$

由此可知設 $a\equiv 0, 1, 2, 4$ 則 $x^2\equiv a\ (mod.\ 7)$ 有一解，若 $a\equiv 3, 5, 6$，卽無解。前者諸數爲諸方之餘 $(mod.\ 7)$，或簡稱 7 之二次餘；後者諸數非是此項餘。

54. 定義 設 $x^2\equiv a\ (mod.\ p)$ 有一解，則 a 稱爲"p之二次餘"，不則稱爲"p之二次非餘"。又，"二次"一字每簡便略去。

55. 我們不難證明，p之二餘之積，亦仍為餘；二非餘之積則為餘；而一餘一非餘之積乃是非餘。

56. 前述結果，若用入萊根德 (*Legendre*) 符號 $\left(\frac{a}{p}\right)$，則可用一方程表之。萊氏符號用法如下：若a為p之餘，則此號之值為$+1$，若a非餘，則其值為-1。於是得：

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)=\left(\frac{ab}{p}\right)。$$

由此可知設$m=(-1)^a 2^b p_1{}^c p_2{}^d\cdots$則

$$\left(\frac{m}{p}\right)=\left(\frac{-1}{p}\right)^a\left(\frac{2}{p}\right)^b\left(\frac{p_1}{p}\right)^c\left(\frac{p_2}{p}\right)^d\cdots$$

57. 欲知一數目m是否為p之餘，祗須決定是否-1,2及m之奇質數的因子為p之餘。下面的結果可證明：

$$I.\quad \left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}。$$

$$II.\quad \left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}。$$

$$III.\quad \left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}。$$

(p,q 爲奇質數)

58. 後者是一重要定理，名爲"萊氏反互律"，如下述之：設 p 與 q 爲二奇質數，而至少其中之一作 $4n+1$ 形式，則 q 爲 p 之餘，祇當 p 爲 q 之餘時纔如此，而如 p 與 q 均作 $4n+3$ 形式，則當 p 爲 q 之非餘時，q 爲 p 之餘，反之亦然。

此定理首爲歐拉 (*Euler*) 由經驗得之，稍後卽由萊氏演爲普通形式，幷部分的證明之。然完全的證，則高斯 (*Gauss*) 始成之，他幷作出八個不同的證。其後幷還有他人證之，至今其證已有數十個了。

用界尺及圓規之作法
有法多角形

L. E. Dickson 著

目　　次

用界尺及圓規之作法有法多角形

L. E. Dickson 著

1. **引言** 古希臘幾何學家發見了用界尺及圓規之作法於各種簡易的問題。然有許多著名的問題，古時人想用此法求其解而未能，例如將一立方二倍之，將一角三等分之，及求圓之平方等。這些作法之不可能，近時始證明之；其證法旣出了初等幾何學之範圍，自必多借助於解析的方法，如代數學上之普通方法及定理。并且有許多作法之可能，亦藉此項解析的方法始發見，例如十七

邊有法多角形，其可用界尺及圓規以作之，自歐几里得(*Euclid*)至高斯(*Gauss*)無人想及的。

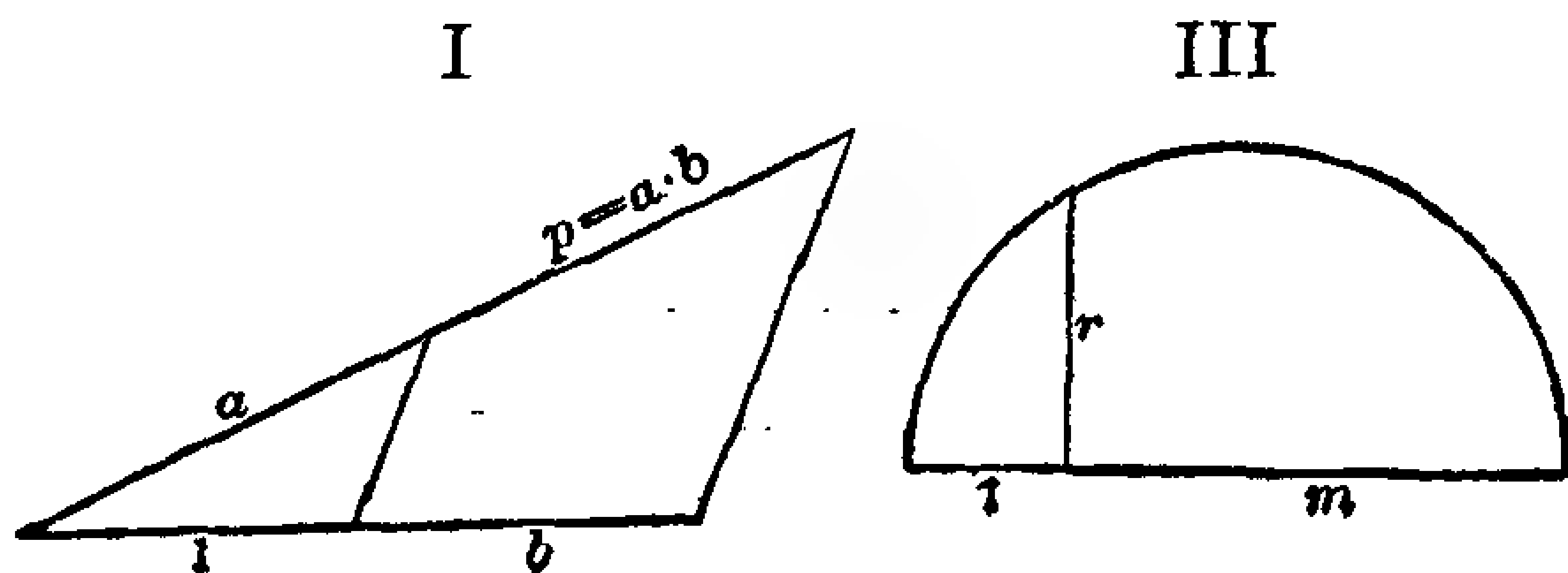
2. 可作性之解析的標準 論一作法之第一步，是將所論問題解析的演出之。在有的例內，初等代數學已够用。例如將一立方二倍之的問題，我們先設一邊長s，而求一數目x，能$x^3=2s^3$者。然尋常用解析幾何學當較省事；點可用其坐標x與y決定之，直線與圓可用一次與二次的方程決定。因此，所關的數目，有的是點之坐標，有的是方程中係數之比，有的則表長，面積或體積。今立以下的

標準 所欲從事的作法，倘(解析的)決定所求之幾何元素的數目，能用有限數的有理算法與開實平方根自決定所設之元素的數目推得，則此作法可用界尺與圓規爲之。

試先假定作法是可能的，則所用直線與圓，由開始時所設的點或由直線與圓等相交的點所決定。二直線之相交點之坐標，乃是二線之方程中係數

之有理函數。欲決定直線$y=mx+b$與圓$(x-c)^2+(y-d)^2=r^2$之交點之坐標，可於二方程中消去y而得一x之二次方程。如是，x(幷$mx+b$或y)除了一某式之方根而外，別無其他無理性可得。又，前面的圓與一其他圓$(x-e)^2+(y-f)^2=s^2$之相交，可得自一圓與其公弦之交，而此弦之方程，則由前者相減得之。因之，此第三例即化爲第二例。標準內所說故即明白。

反之，設如除實平方根以外無其他無理性，則其作法可用界尺與圓規爲之。第一，所設的數量之有理函數可由加，減，乘，除得之。作二段(*segments*)之和或差，這是很明白的；作二段之積與商，則如*I*圖與*II*圖中所示；至作一段，其長爲$r=\sqrt{m}$，則可如*III*圖爲之。



3. 二次方程之圖解法 方程

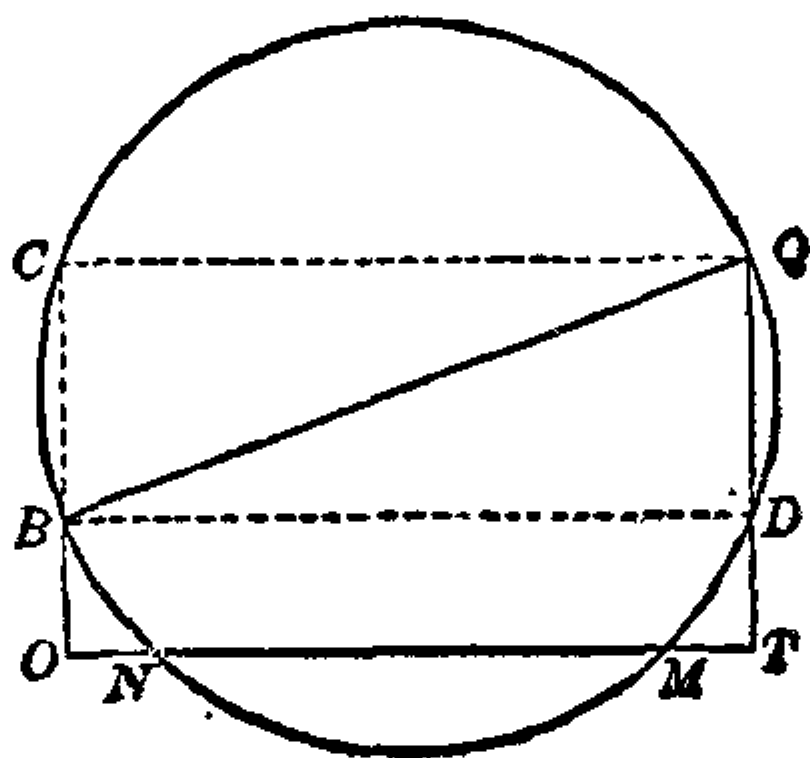
$$x^2-ax+b=0$$

之根乃是 $\frac{1}{2}(a\pm\sqrt{a^2-4b})$。如根爲實，則祇能有實平方根之無理性，故可滿足前節之標準。諸作法中以下面者爲尤簡：

作一以 BQ 線爲徑的圓此線連 $B=(0,1)$ 與 $Q=(a,b)$ 二點。則此圓與 x 軸之二交點之坐標 ON 與 OM 卽爲 $x^2-ax+b=0$ 之根。

〔證1〕 如下圖內，$OB=1$，$OT=a$，$TQ=b$。故圓之心爲 $\left(\frac{a}{2},\ \frac{b+1}{2}\right)$，其徑爲 BDQ 直角三角形之弦。故此圓之方程是

$$\left(x-\frac{a}{2}\right)^2+\left(y-\frac{b+1}{2}\right)^2=\left(\frac{a}{2}\right)^2+\left(\frac{b-1}{2}\right)^2。$$



欲求其與 x 軸之交點，可設$y=0$，而得 $x^2-ax+b=0$。

〔證2〕用初等幾何學證之，可設 OB 再遇圓於 C，TQ 遇圓於D。連CQ與BD。因BQ是徑，C與 D 爲直角。故 $OC=b$，$DT=OB$。因平行線含等弧，故BN與DM弦相等，而BON與DTM二三角相合，$ON=MT$。於是 $OM+ON=OM+MT=OT=a$。但

$$OM\cdot ON=OC\cdot OB=b\cdot 1=b,$$

故OM與ON卽是$x^2-ax+b=0$之根。

4. 有理性領域 設如一組數目有此屬性，用每一有理演算法，加，減，乘，除（不能用0爲除數）施於其任何二數目上，所得者仍爲此組內之數目，此組數目卽名"有理性領域"。

例如一切實數所成的組是一有理性領域，因任何二實數之和，差，積，商乃是一實數。又，一切有理數（一切正與負的整與分數）之組是一有理性領域。惟一切正整數之組非是，蓋二正整數之

差不必定爲正整數。卽一切正與負的整數所成的組亦然，因二整數之商，不必定爲整。而一切有理函數，其係數爲整的，由指定的數目 $a,b,c,\cdots$ 所成，亦一有理性領域；而云爲 $a,b,\cdots$ 所“定”。

所欲從事的作法內，所設的幾何元素爲 $a,b,\cdots$ 所解析的決定，則由 $a,b,\cdots$ 所定的有理性領域，名爲“幾何張本領域”，而用 D 表之。

5. 除平方根外無其他無理性的函數 設 x 爲一函數，用有理算法及開平方自 D 中 $a,b,\cdots$ 得之。則研究此項函數之用意，在得一可作性條件，較之 2 節中標準尤易用。

x 之項內重疊的根號之數，名爲此項之“次”；其最大的次用 m 表之。例如 $x=\sqrt{\sqrt{a}+\sqrt{b}+\sqrt{c+\sqrt{d}}}+\sqrt{\sqrt{e}+\sqrt{f}+g}$ 內，前三項爲 2 次者，第四項1次，末項 g 0 次；故 $m=2$。但往往一函數可變其形使次數低些；例如 $\sqrt{9}$ 可寫作 3，$\sqrt{10-2\sqrt{3}}$ 寫作 $\sqrt{3}-1$。設 $r=\sqrt{3+\sqrt{5}}$，而

$r'=\sqrt{3-\sqrt{5}}$，則 $rr'=2$，而 $2r-7r'$ 包括二2次的根者，可用$2r-\frac{14}{r}$代之，此則祇有一2次的根了。又設x有$\sqrt{3}$，$\sqrt{5}$與$\sqrt{15}$，則可用$\sqrt{3}\cdot\sqrt{5}$代$\sqrt{15}$。廣之，設任何一n次的根，乃是其餘n次的根及較低次者之有理函數，則假定其用其他根表出之。故使其簡單以後，各種m次的根中沒有一個乃是其餘m次根及較低次的根，分開的遇見或在他根號以下者，之有理函數；彷此，沒有一$m-1$次的根乃是其餘$m-1$者及較低次者之有理函數，等等。x 如此化成簡單後所有不同的根，名爲"獨立的"。

若所得x函數是數個分數之和，則化之成公分母，而將x表作二根之整函數之商。例如$x=\sqrt{5}+2r-\frac{14}{r}$ $(r=\sqrt{3+\sqrt{5}})$，可使x成$\frac{A}{r}$形式$[A=r\sqrt{5}+2(3+\sqrt{5})-14]$。

其次，可將分母用下法化之成有理：設分母有一根$\sqrt[m]{k}$次者，則可使之作$a+b\sqrt[m]{k}$形式(a與

b 無 $\sqrt{k}$)。於是用 $a-b\sqrt{k}$ 乘分子并分母。仿此，可除去分母之每一 m 次的根，及 $m-1$ 者，等。如前例內 $x=\frac{A}{r}$ ($r=\sqrt{3+\sqrt{5}}$)，其第一步得

$$x=\frac{A(-r)}{r(-r)}=\frac{-Ar}{-3-\sqrt{5}},$$

第二步得 $$x=\frac{-Ar(-3+\sqrt{5})}{(-3-\sqrt{5})(-3+\sqrt{5})}$$

$$=\frac{3Ar-Ar\sqrt{5}}{4}。$$

如是已證明，x 可成爲正則的形式，由諸項之和所成，每個爲根數之積，以 D 中一數爲係數，而分開的根是獨立的。

例如 $5+\frac{2}{3}\sqrt{5}-\frac{1}{2}\sqrt{7}+4\sqrt{5}\sqrt{7}$ 是正則的形式。

6. 設 n 爲不同的根數（包括根號下的根）之數，在 x 之正則形式中者。將 n 根數中之一或數個遍易其號，卽得 2^n 個"共軛"函數 $x=x_1, x_2, \cdots, x_{2^n}$。例如 $x_1=\sqrt{3+2\sqrt{5}}+\sqrt{3-2\sqrt{5}}$ 卽是 $2^3=8$

個共軛者中之一，此中祇四個是不同的。即：

$x_1,x_2=\sqrt{3+2\sqrt{5}}-\sqrt{3-2\sqrt{5}}$, $x_3=-\sqrt{3+2\sqrt{5}}+\sqrt{3-2\sqrt{5}}$, $x_4=-\sqrt{3+2\sqrt{5}}-\sqrt{3-2\sqrt{5}}$。此 2^n 共軛數，$x_1,x_2,\cdots$ 乃是

$$F(x)=(x-x_1)(x-x_2)\cdots(x-x_{2^n})=0$$

之根。此方程之展開式爲

$$F(x)=x^{2^n}+k_1x^{2^n-1}+\cdots+k_{2^n},$$

於此 $k_1=-(x_1+x_2+\cdots+x_{2^n})$， $k_2=x_1x_2+x_2x_3+x_1x_3+\cdots$ 例如 $x=3a+2\sqrt{b}$ 及其共軛 $3a-2\sqrt{b}$ 乃是 $x^2-6ax+9a^2-4b=0$ 之根，其係數在 a 與 b 所定的領域內。

雖然 $x_1,x_2,\cdots$ 有根數，其相稱的結合 k_i 可見其等於無這些根數的式，故爲 $a,b,c\cdots$ 之有理函數，係數爲整的。假如 k_i 有一根數 $\sqrt{r}$，則可使其成 $k_i=p+q\sqrt{r}$ 形式（p 與 q 均無 $\sqrt{r}$）。當此 n 個不同的根數中之任何其一改變了號，$x_1,x_2,\cdots$ 兩兩互換，而 $F(x)$ 仍無變動。因 $\sqrt{r}$ 改爲 $-\sqrt{r}$ 時 k_i 仍

無變動，卽得

$$p+q\sqrt{r}=p-q\sqrt{r},\quad q=0,$$

而 $k_i=p$ 無有$\sqrt{r}$。因k_i無有任何一根數，故等於D中一數目。故函數x滿足一方程$F(x)=0$，其次數2^n，係數在D中。

7. x_1 能滿足各種方程其係數在D中者；例如$M(x)\cdot F(x)=0$，這裏$M(x)$爲任何整函數係數在D內。次卽證明這些方程之一重要屬性。

定理 設 $x_1, x_2, \cdots x_{2^n}$ 諸共軛數中之一滿足任何一方程$f(x)=0$係數在D中者，則一切數 x_i 滿足此方程。

設 $x_1=p+q\sqrt{r}$ ($\sqrt{r}$ 爲最大次m者，p與q不包有$\sqrt{r}$但可有其餘m次或較低次的根數)，將$\sqrt{r}$易其號，卽得一其他x_i，例如$x_2=p-q\sqrt{r}$。$f(x_1)$可使其作$A+B\sqrt{r}$形式，這裏A與B無有$\sqrt{r}$。照所設，$f(x_1)=0$；卽，$A+B\sqrt{r}=0$。如$B\neq0$，則得$\sqrt{r}=\dfrac{-A}{B}$，與假定根數獨立相違。故 $B=0$，而$A=0$。因$f(x_2)=A-B\sqrt{r}$，可得$f(x_2)=0$。此

卽是 x_2 是 $f(x)=0$ 之根。

用此原理，可證任何 x_i 乃是 $f(x)=0$ 之根。爲簡單計，可設 x_1 恰含二根數 $\sqrt{r}$ 與 $\sqrt{r'}$，爲 m 次者。於是(5節末)

$$f(x_1)=A+B\sqrt{r}+C\sqrt{r'}+E\sqrt{r}\sqrt{r'},$$

這裏 A,B,C,E 祇小於 m 次的根數。因根數之獨立性，可見 A,B,C,E 必均爲0。今設 A 有三根數 $\sqrt{s}$, $\sqrt{s'}$, $\sqrt{s''}$ 爲 $m-1$ 次者，則 $A=g+h\sqrt{s}+i\sqrt{s'}+j\sqrt{s''}+k\sqrt{ss'}+\cdots+q\sqrt{s}\sqrt{s'}\sqrt{s''}$。如前，$A=0$，卽使 $g,h,\cdots,q$ 亦爲0。仿此，B,C,E 內亦然。其他 $m-2,\cdots,1$ 各次的根數亦可如是爲之。因之，

$f(x_1)=d+e\sqrt{r}+f\sqrt{r'}+g\sqrt{s}+\cdots+p\sqrt{r}\sqrt{r'}+q\sqrt{r}\sqrt{s}+\cdots+t\sqrt{r}\sqrt{r'}\sqrt{s}+\cdots$ 中每個係數 $d,e,f,\cdots$ 爲0。因 x_i 可用改變某個根數 $\sqrt{r}$, $\sqrt{r'}$, $\sqrt{s}\cdots$ 之號之法自 x_1 得之，故 $f(x_i)$ 亦可如是由前 $f(x_1)$ 式內得之。$d, e, f,\cdots$ 旣爲0，故 $f(x_i)$ 爲0。於是 x_i 爲 $f(x)=0$ 之根。

8. 6節內曾指出，x_1 滿足一方程 $F(x)=0$ 其次數爲 2^n 係數則在 D 內。此項方程內，今設其一次數至低者，爲 l 次的，作 $\phi(x)=0$，而 x^l 之係數則可假定其爲1。如是 l 次的方程不能有二，因相減時卽可得一次數小於 l 的方程，係數在 D 內，根爲 x_1。

今可證明 $F(x)$ 乃是 $\phi(x)$ 之乘方。用 $\phi(x)$ 除 $F(x)$，并假定其商爲 $F_1(x)$，餘爲 $r(x)$ 次數小於 l（$F_1(x)$ 與 $r(x)$ 爲整函數，係數在 D 內）。則 $F(x)=\phi(x)\cdot F_1(x)+r(x)$。設 $x=x_1$，因 $F(x_1)=0$，$\phi(x_1)=0$，卽 $r(x_1)=0$。如 $r(x)$ 非爲0，則 $r(x)=0$ 之係數在 D 內，其根爲 x_1，次數小於 l 者，此卽違所設 l 爲此項方程之最低次的假設。故 $r(x)$ 爲0，而 $F(x)=\phi(x)\cdot F_1(x)$。

如 $F_1(x)$ 爲一常數，必係1，$F(x)$ 卽爲 $\phi(x)$ 之一次方，於是所說的定理證明了。反之，$F_1(x)$ 爲 $F(x)$ 之因子次數大於或等於1，而 $F_1(x)=0$ 至少有 $F(x)=0$ 之一根 x_i 爲根，故（7節）卽有每個 x_i

爲根。詳之，$F_1(x)=0$有x_1爲根，故由前證法，

$$F_1(x)=\phi(x)\cdot F_2(x),$$

這裏$F_2(x)$爲整函數係數在D內。如$F_2(x)$化爲常數，必爲1，$F(x)$卽爲$\phi(x)$之平方；定理亦卽證明了。反之，同前的證法可明

$$F_2(x)=\phi(x)\cdot F_3(x)。$$

如是下去，可得　　$F(x)=[\phi(x)]^k$。

此式右端之次爲 lk，而左端爲2^n，故 l 爲 2^n 之除數，而$\phi(x)$之次數爲 2 之乘方。於是我們得下定理：

不二的最低次的方程，係數在 D 內，而爲(由 D 中數目用有限數有理算法及開平方法推得的)函數x_1所滿足者，其次數爲 2 之乘方。

9. 可化與不可化的函數　一整函數$f(x)$其係數在D內者，視其能否化爲二整函數（每個均爲$\geqq 1$次者，係數亦在D內）而名爲在此領域內可化的或不可化的。例如x^2-4於任何領域內均可化；x^2-3在有理數領域內不可化，在實數領域內可

化；x^2+4 在後者內不可化，但在一切實數與虛數領域內可化，因

$$x^2+4=(x+2i)(x-2i)\quad(i=\sqrt{-1})。$$

10. 8節內所定的 $\phi(x)$ 在 D 內不可化。蓋設 $\phi(x)$ 爲二整函數之積，每個次數均爲 $\geqq 1$，係數在 D 內，則當一因子使其等於 0 時將得一方程，其係數在 D 內，而爲 x_1 所滿足，次數則小於 $\phi(x)$。然此即違關於 $\phi(x)$ 之假設。

一方程 $G(x)=0$ 名爲在 D 內不可化者，假如函數 $G(x)$ 於 D 內不可化。方程 $\phi(x)=0$ 乃是惟一在 D 中不可化者，其根爲 x_1。蓋設 $G(x)=0$ 在 D 內不可化，其根爲 x_1，則8節內所用論證法證明 $G(x)$ 有因子 $\phi(x)$，故 $G(x)$ 必爲 $\phi(x)$ 與一常數之積。故8節定理等於下面者：

不二的在 D 中不可化的方程，爲（由 D 中數目用有限數有理算法與開平方法推得的）函數 x_1 所滿足者，其次數爲 2 之乘方。

11. 由此定理及2節之標準，即得一

根本定理　一所欲從事的作法，倘(解析的)決定所求之幾何元素的數目中任何一個能滿足一在D中不可化的方程其次數非爲2之乘方者，則此作法不能用界尺與圓規爲之。

12.　由前面的結果，乃可研究引言中所述三著名的問題。

倍一立方　此問題卽是欲求一立方，其體積倍於一已知的立方。將已知的立方之一邊取爲長之單位，則可知所求的立方之一邊x，乃是$x^3=2$之根。$x^3-2=0$於有理數領域內不可化；蓋若可化，則能有一次的因子，因而有有理根了。設$\frac{a}{b}$爲一根(a與b爲整數無公除數)，則$a^3=2b^3$。故a^3幷a爲偶的，$a=2c$。於是$4c^3=b^3$，而b爲偶的。因之，a與b均爲偶，而有公因子2，此卽違所設者。因$x^3=2$之次數非爲2之乘方，故由前節知此問題不能用界尺與圓規解之。

角之三等分　欲證明一隨意的角，不能用界尺與圓規三分之，祇須證明一特例如$120°$角便行.

(註：有的特例如 360°, 180°, 90° 的角，可三分之，因 120°,60°,30° 的角可用界尺與圓規爲之)。作一 40° 的角，等於作一直角三角形，其弦爲1，底爲 $\cos 40°$。照三角學，$\cos 3x = 4\cos^3 x - 3\cos x$，而 $\cos 120° = -\frac{1}{2}$，故

$$4\cos^3 40° - 3\cos 40° + \frac{1}{2} = 0。$$

用2乘之，并設 $y = 2\cos 40°$，得

$$y^3 - 3y + 1 = 0。$$

此方程於有理數領域內不可化。蓋若可化，則有一次的因子并一根 $\frac{a}{b}$ (a與b爲整數，無公因子，b 爲正的)。今設 $y = \frac{a}{b}$，并用 b^2 乘，得

$$\frac{a^3}{b} - 3ab + b^2 = 0,$$

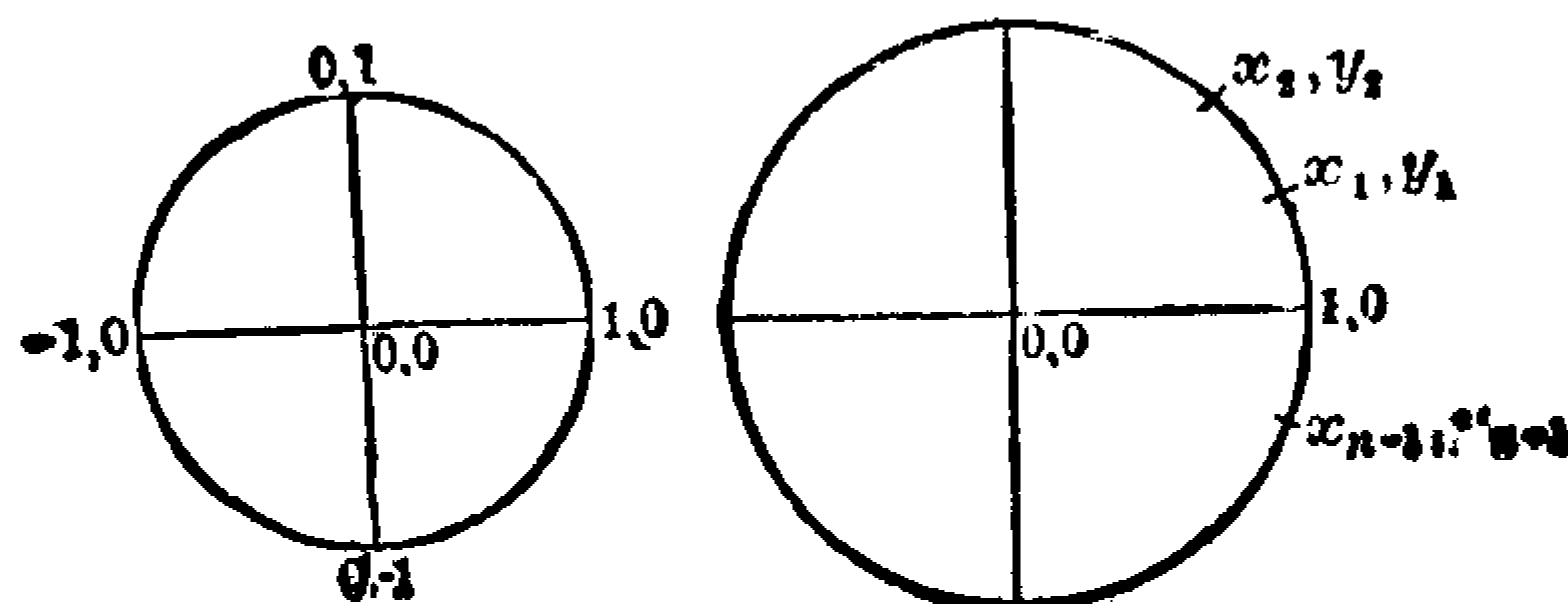
而 $\frac{a^3}{b}$ 爲一整數。設$b>1$，a與 b 卽有公因子>1。故 $b=1$。整根$y=a$使a^3-3a成爲 a 之整倍數，故方程中常數項1，必爲 a 之倍數。於是 $a=\pm 1$。由試驗可知$+1$與-1均不能爲此方程之根；故照

11節，三分120°角不能用界尺與圓規爲之。

又，9 邊有法多邊形不能用界尺與圓規切入圓內，故此問題不可能。

求圓之平方 此問題在用界尺及圓規作一平方，其面積等於一以 R 爲半徑的已知圓之面積πR^2。此項作法不可能。蓋若可能，則可取R爲單位，而π能滿足一有理係數的代數方程了。然此是不能者(參觀第九篇)。

13. 有法多邊形與一之根間之關係 試論一n邊有法多邊形切於一單位圓內者。我們用直角坐標系，起點在圓心，而x軸過多邊形之一角。此頂角點之坐標爲 (1,0)。若爲四邊形，則其餘頂點之坐標如下圖所示。若n爲任何數，則其餘諸頂點如下右圖中所示，表之爲$(x_1, y_1)\cdots$，$(x_{n-1},$



y_{n-1})。因 n 邊形每邊所對在心之角其量爲 $\frac{2\pi}{n}$，故 $x_1=\cos\frac{2\pi}{n}$，$y_1=\sin\frac{2\pi}{n}$，$x_2=\cos\frac{4\pi}{n}$，$y_2=\sin\frac{4\pi}{n}$，等等。平面內每一點 (x,y) 不二的決定一雜數 $x+iy$ $(i=\sqrt{-1})$。

反之，亦然。故四邊形之各頂點，其雜數爲：

$$1,i,-1,-i \tag{1}$$

而 n 邊形之各頂點，其雜數爲：

$$\left.\begin{aligned}&1, r_1=\cos\frac{2\pi}{n}+i\sin\frac{2\pi}{n}, r_2=\cos\frac{4\pi}{n}+i\sin\frac{4\pi}{n},\\ &\cdots r_{n-1}=\cos\frac{2(n-1)\pi}{n}+i\sin\frac{2(n-1)\pi}{n}。\end{aligned}\right\}\tag{2}$$

因 $i^2=-1$，故 (1) 之四數乃是以下方程之根：

$$x^4=1 \tag{3}$$

而卽名爲1之四次根。(2) 中任何一數乃是以下方程之根：

$$x^n=1, \tag{4}$$

故名爲1之 n 次根。蓋因

$$r_k=\cos\frac{2k\pi}{n}+i\sin\frac{2k\pi}{n}, \tag{2'}$$

故用後面的公式(5)，知 $r_k^n = \cos 2k\pi + i \sin 2k\pi = 1 + i \cdot 0 = 1$。

14. 德摩夫爾 (de Moivre) 定理 倘n爲任何正整數，卽得

$$(\cos A + i \sin A)^n = \cos nA + i \sin nA \qquad (5)$$

我們可先證此式:

$$(\cos A + i \sin A)(\cos B + i \sin B) = \cos(A+B) + i \sin(A+B)。 \qquad (6)$$

設$a = \cos A \cos B - \sin A \sin B = \cos(A+B)$，$b = \cos A \sin B + \sin A \cos B = \sin(A+B)$，則前積卽作$a+ib$式。倘於(6)內使$B=A$，卽得$n=2$的(5)；於$n=1$，(5)自然無誤。故用數學上的歸納法，卽[illegible]之至於任何指數n。我們可假定於$n=m$無誤，卽

$$(\cos A + i \sin A)^m = \cos mA + i \sin mA,$$

則可用$\cos A + i \sin A$乘其兩端，而用(6)以得右端之積，則得

$$(\cos A + i \sin A)^{m+1} = \cos(m+1)A + i \sin$$

$(m+1)A$;

如是，於 $n=m+1$ 亦無誤，而(5)之歸納的證全了。

15. 由德氏定理，知前面之(2')，乃是

$$r=\cos\frac{2\pi}{n}+i\sin\frac{2\pi}{n} \tag{7}$$

之 k 次方。故(2)可作以下形式：

$$1=r^n, r_1=r, r_2=r^2, \cdots, r_k=r^k, \cdots, r_{n-1}=r^{n-1}。$$

因這 n 個數目是不同的，而是(4)之根，故卽爲(4)之一切根。一代數方程之 n 次者，其根亦不能多於 n 個(見第五篇10節)。75頁右圖單位圓內所切有法 n 邊形之各頂角，可表 n 個分開的數目

$$1, r, r^2, \cdots r^k, \cdots r^{n-1} \tag{8}$$

爲1之一切 n 次根者。這裏 r 爲(7)所定。

如 $n=4$，這些數目卽是 $1, i, i^2=-1, i^3=-i$。

16. 雜數 $C=\cos A+i\sin A$ 之倒數爲 $C^{-1}=\cos A-i\sin A$，因此二者相乘之積爲 $\cos^2A+\sin^2A=1$，其和 $C+C^{-1}$ 則爲 $2\cos A$。

用界尺與圓規切入一有法 n 邊形，等於作一 $\frac{2\pi}{n}$

的角，卽等於作一直角三角形，弦爲1，底爲 $\cos\frac{2\pi}{n}$ 者。所以我們不必決定 r[如前(7)所定者]之雜根，祇須決定 $r+r^{-1}=2\cos\frac{2\pi}{n}$ 便行。因 $r^n=1$，故 $r^{-1}=r^{n-1}$。於是可求(8)之某個實值的結合，如 $r+r^{n-1}$ 者。

17. 有法五邊形與十邊形 於 $n=5$，今欲決定

$$\eta_0=r+r^4=2\cos\frac{2\pi}{5}\quad\left(r=\cos\frac{2\pi}{5}+i\sin\frac{2\pi}{5}\right)。$$

因 $r^5=1$，$r\neq1$，卽得

$$\frac{r^5-1}{r-1}=r^4+r^3+r^2+r+1=0。$$

故若 $r+r^4$ 求得，則亦得 $\eta_1=r^2+r^3$，因 $\eta_0+\eta_1=-1$。二數目之和與積已知，則卽能決定其値。故可計算 $\eta_0\cdot\eta_1$。相乘，得

$$(r+r^4)(r^2+r^3)=r^3+r^4r^6+r^7=r^3+r^4+r+r^2=-1。$$

由此知 η_0 與 η_1 乃是 $x^2-(\eta_0+\eta_1)x+\eta_0\eta_1\equiv x^2+x-1=0$ 之根 $\frac{1}{2}\left(-1\pm\sqrt{5}\right)$。

因銳角之 cos 是正的，卽得

$$\eta_0=2\cos\frac{2\pi}{5}=\frac{1}{2}(-1+\sqrt{5}),\ \eta_1=\frac{1}{2}(-1-\sqrt{5})。$$

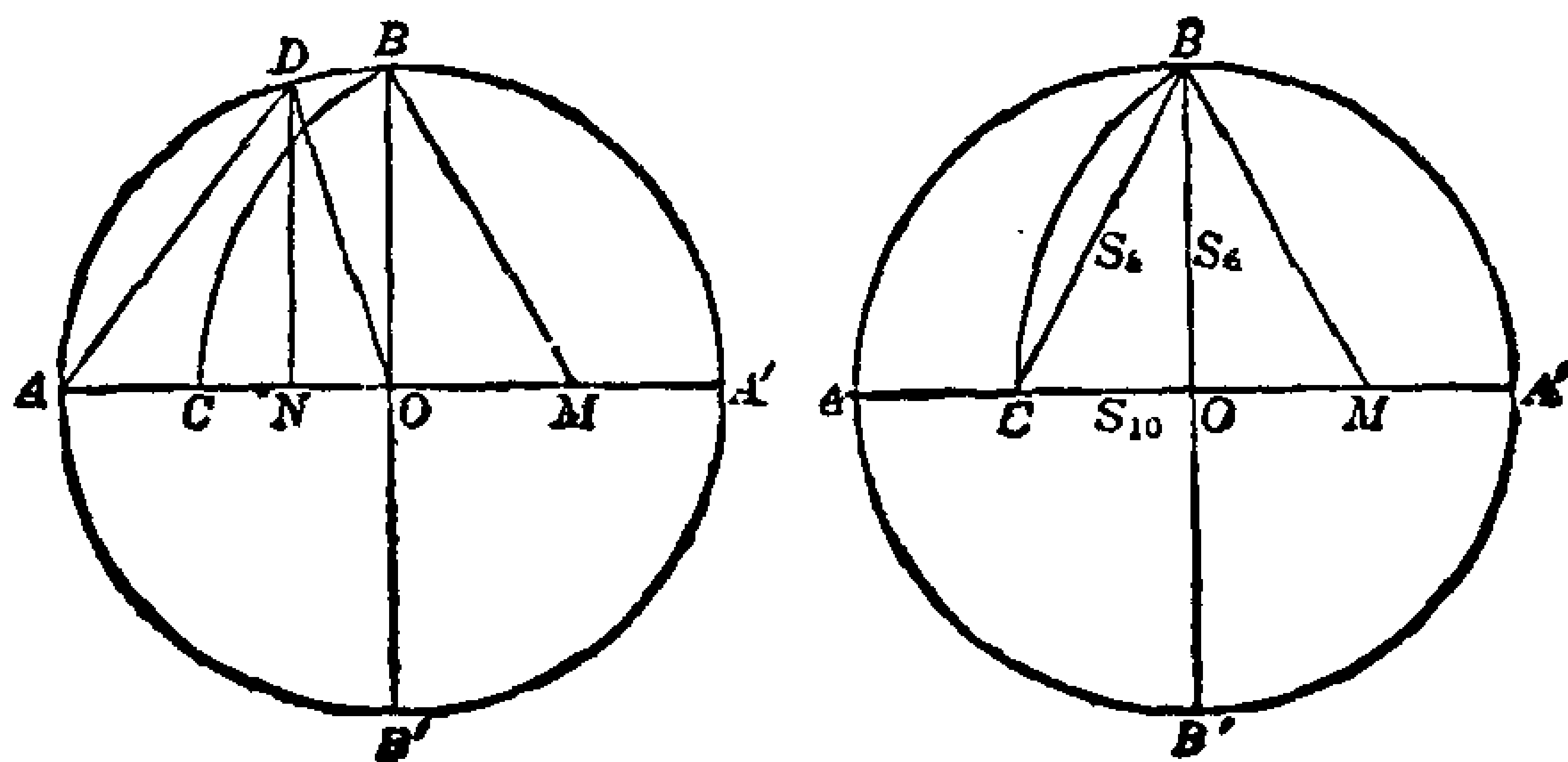
由此 η_0 之値，卽可作 $\frac{2\pi}{5}$ 的角。設 AOA' 與 BOB' 爲 R 半徑的圓內之相乘直的徑，M 爲 OA' 之中點(如下左圖)。則

$$BM^2=R^2+\left(\frac{1}{2}R\right)^2,\ BM=\frac{1}{2}R\sqrt{5}。$$

今以 M 爲心，BM 爲半徑作圓，交 OA 於 C，而 N 爲 OC 之中點，則

$$OC=\frac{1}{2}R(\sqrt{5}-1)=R\eta_0,\ ON=R\cos\frac{2\pi}{5}。$$

作 DN 與 OB 平行，DON 角等於 $\frac{2\pi}{5}$，故 AD 卽



是內切五邊形之邊S_5。

今可略去DN, DO, DA，而證明$CB=S_5$，CO等於一有法十邊形之邊S_{10}。

蓋 $$S_{10}=2R\sin 18^0=2R\cos 72^0\equiv 2R\cos\frac{2\pi}{5}=$$

$$R\eta_0=OC。$$

其次，$\sin 18^0=\cos 72^0=1-2\sin^2 36^0$。用$2R^2$乘之，而以$S_5$代$2R\sin 36^0$，$S_{10}$代$2R\sin 18^0$，卽得

$$Rs_{10}=2R^2-S_5^2。$$

但η_0爲$x^2+x-1=0$之根，而$R\eta_0=S_{10}$，故

$$S_{10}^2+Rs_{10}-R^2=0。$$

而 $$S_{10}^2+R^2=S_5^2。$$

因$OC=S_{10}$，$OB=R$，故$BC=S_5$。於是得

設AOA'與BOB'爲相垂直的徑，M爲半徑OA'之中點，則以M爲心MB爲半徑的圓交OA於C，而OC與BC卽是內切有法十邊與五邊形之邊S_{10}與S_5。

前面右圖，顯出內切十邊，六邊，及五邊形之邊間之關係：$S_{10}^2+S_6^2=S_5^2$。

18. 設p為質數，則p邊有法形可用界尺與圓規為之，此不僅於$p=3,5$如此，即$p=17$及其他較大的值亦然。此為高斯所發見，其普通定理見27節。

前節內論$p=5$時，曾用過$r+r^4$與r^2+r^3，名為"週期"。設後者作$r,r^2,r^4,r^3=r^8$次序寫之，俾每個為其前之方，則可見取其等值的項時，即得週期。對於p之其他值，或即不能將1之p次諸雜根$r,r^2,r^3,\cdots,r^{p-1}$, (9)

列成如是次序，使每項為其前者之平方。事實上，$p=7$即不能如此，因第四項r^8與第一項r同，但若使每項為前者之立方，即行：

$$r,r^3,r^2,r^6,r^4,r^5。$$

第七篇46節曾指出，對於任何質數p有一整數g(名p之質根)，用p除$1,g,g^2,\cdots g^{p-2}$所得餘數作某種次序$1,2,\cdots p-1$。故

$$r,r^g,r^{g^2},\cdots r^{g^{p-2}} \tag{10}$$

諸根與(9)以某種次序相同。

19. 有法17邊形 於$p=17$，可取$g=3$，因用17除3之各方 $1,3,3^2,\cdots 3^{16}$，其餘數爲

$$1,3,9,10,13,5,15,11,16,14,8,7,4,12,2,6,$$

乃是$1,2,\cdots 16$之一個變互。試取其變易的項，得週期

$$\eta_0=r+r^9+r^{13}+r^{15}+r^{16}+r^8+r^4+r^2,$$

$$\eta_1=r^3+r^{10}+r^5+r^{11}+r^{14}+r^7+r^{12}+r^6。$$

因$r^{17}=1$，$r\neq 1$，卽得

$$\frac{r^{17}-1}{r-1}=r^{16}+r^{15}+\cdots+r+1=0。$$

從可知 $\eta_0+\eta_1=-1$。將二者相乘，卽 $\eta_0\eta_1$，得64項，而用$r^{17}=1$以化去大指數，可知每一根 r，$r^2,\cdots r^{16}$ 恰遇見四次。故

$$\eta_0\eta_1=4(r+r^2+\cdots+r^{16})=-4。$$

但η_0,η_1 爲 $x^2-(\eta_0+\eta_1)x+\eta_0\eta_1=0$之根。故 η_0 與 η_1 滿足

$$x^2+x-4=0 \tag{11}$$

於η_0內及η_1內取變易的項，卽可各得二週期：

$$\eta_0'=r+r^{13}+r^{16}+r^4,\ \eta_2'=r^9+r^{15}+r^8+r^2,$$

$(\eta_0=\eta_0'+\eta_2')$。

$\eta_1'=r^3+r^5+r^{14}+r^{12}$, $\eta_3'=r^{10}+r^{11}+r^7+r^6$,

$(\eta_1=\eta_1'+\eta_3')$。

我們容易明白$\eta_0'\eta_2'=-1=\eta_1'\eta_3'$。故

$$\eta_0',\ \eta_2' \text{ 滿足 } x^2-\eta_0x-1=0 \qquad (12)$$

$$\eta_1',\ \eta_3' \quad ,, \quad x^2-\eta_1x-1=0 \qquad (13)$$

照16節所說，祇須決定$r+r^{16}$便行。$\eta_0''=r+r^{16}$, $\eta_4''=r^{13}+r^4$之和爲η_0'，積爲η_1'，故η_0''，η_4''滿足$x^2-\eta_0'x+\eta_1'=0$ (14)

欲決定(11)之何根是η_0，何根是η_1，以及(12)－(14)內之相仿的問題，可用下式：

$$r=\cos\frac{2\pi}{17}+i\sin\frac{2\pi}{17},\quad r^k=\cos\frac{2k\pi}{17}+i\sin\frac{2k\pi}{17}。$$

故可知 $\eta_0''=2\cos\frac{2\pi}{17}$, $\eta_4''=2\cos\frac{8\pi}{17}$, $\eta_0''>\eta_4''$。

而用 $\cos\frac{10\pi}{17}=-\cos\frac{7\pi}{17}$ 時，可得

$$\eta_0'=2\cos\frac{2\pi}{17}+2\cos\frac{8\pi}{17},\quad \eta_1'=2\cos\frac{6\pi}{17}-2\cos\frac{7\pi}{17}。$$

故η_0'與η_1'是正的。又

$$\eta_1 = 2\cos\frac{6\pi}{17} - 2\cos\frac{5\pi}{17} - 2\cos\frac{7\pi}{17} - 2\cos\frac{3\pi}{17}$$

是負的，因首項小於次項。但 $\eta_0\eta_1 = -4$，故 η_0 是正的，而由(11)－(14)知

$$\eta_0 = \frac{1}{2}(\sqrt{17}-1), \quad \eta_1 = \frac{1}{2}(-\sqrt{17}-1),$$

$$\eta_0' = \frac{1}{2}\eta_0 + \sqrt{1+\frac{1}{4}\eta_0^2},$$

$$\eta_1' = \frac{1}{2}\eta_1 + \sqrt{1+\frac{1}{4}\eta_1^2}。$$

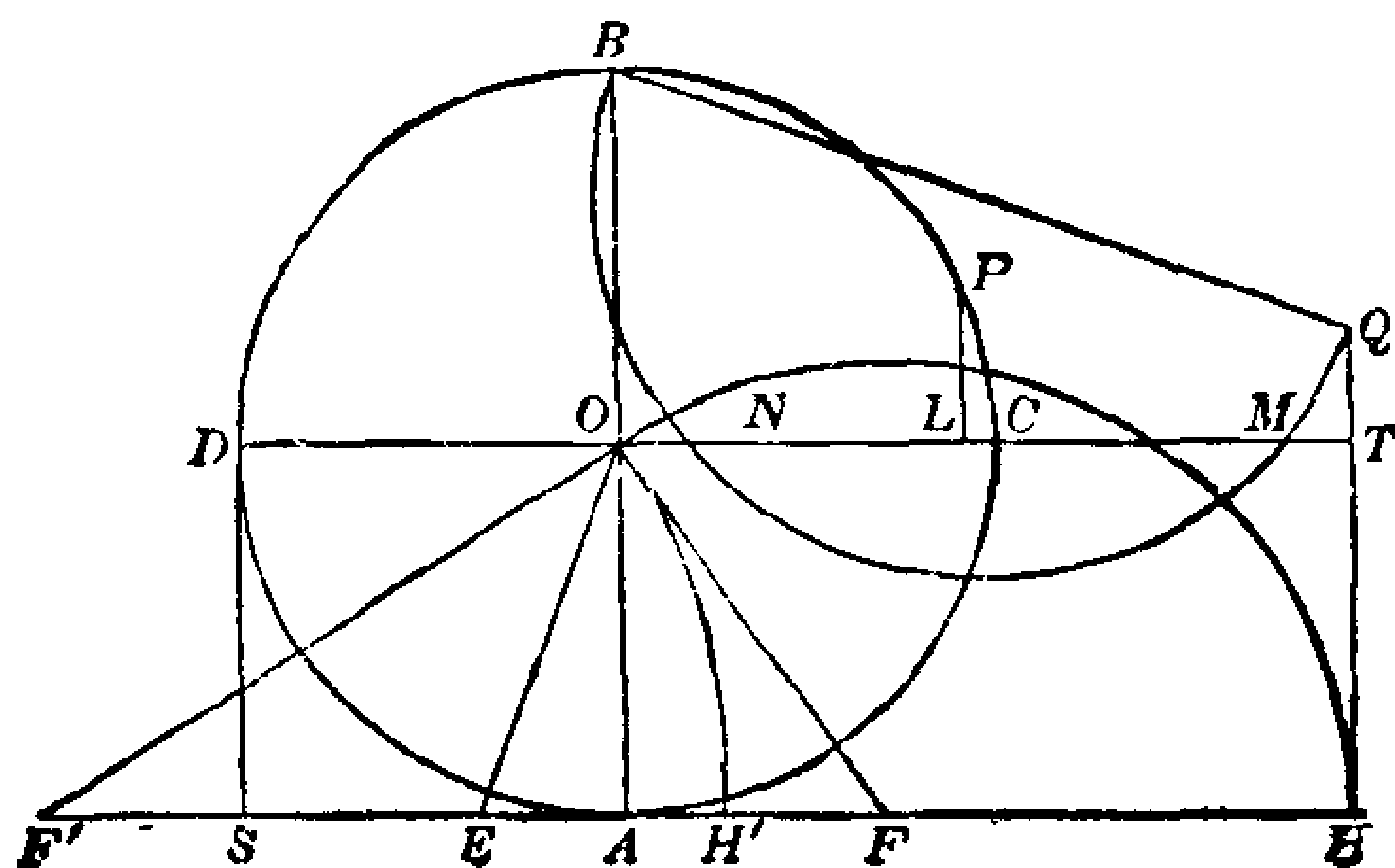
20. 有法 17 邊形之作法 於單位圓內作二垂直的徑 AB, CD，A 與 D 點作二切線相交於 S。試決定 E 點，俾 $AE=\frac{1}{4}AS$，則 $AE=\frac{1}{4}$， $OE = \sqrt{AO^2+AE^2} = \frac{1}{4}\sqrt{17}$。以 E 為心，OE 為半徑，作圓交 AS 於 F 及 F'。則 $AF=EF-EA=OE-\frac{1}{4} = \frac{1}{2}\eta_0$， $AF'=EF'+EA=OE+\frac{1}{4} = -\frac{1}{2}\eta_1$，$OF=\sqrt{AO^2+AF^2}=\sqrt{1+\frac{1}{4}\eta_0^2}$， $OF'=\sqrt{1+\frac{1}{4}\eta_1^2}$。又以 F 為心 FO 為半徑作圓交 AS 於

H；以F'爲心$F'O$爲半徑交AS於H'，則$AH=AF+FH=AF+FO=\frac{1}{2}\eta_0+\sqrt{1+\frac{1}{4}\eta_0^2}=\eta_0'$，

$$AH'=F'H'-F'A=OF'-AF'=\eta_1'。$$

此外，再須作(14)之根，此則可照3節爲之。作HTQ與AO平行，交OC於T。使$TQ=AH'$。將$B=(0,1)$與$Q=(\eta_0',\eta_1')$相連，而以BQ爲徑作圓，則此圓與x軸OT相交的點ON與OM，即是(14)之根。故較大的根η_0''爲$OM=2\cos\frac{2\pi}{17}$。

OM之垂直的平分線LP交單位圓於P。而$\cos LOP=OL=\cos\frac{2\pi}{17}$，即$LOP=\frac{2\pi}{17}$。故$CP$弦即是內切十七邊形之一邊。



21. 既論過 $p=5$, 17二特例, 可闡述高斯之任何質數p的理論。

設 $p-1=ef$ 爲 $p-1$ 之任何一種因子分解法, 我們可將 $p-1$個根(10), 分爲 e 組, 每組 f 個。第一組內有第一根r, 繼之者爲第e個根 r^{g^e}, 於是又繼之以第 e 個根, 等等。第二組有第二根 r^g, 繼之者爲第 e 個根, 等等。各組內之指數於是如下

$$\left.\begin{array}{l} 1,\ g^e,\ g^{2e},\cdots\cdots\cdots g^{(f-1)e} \\ g,\ g^{e+1},\ g^{2e+1},\cdots g^{(f-1)e+1} \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ g^{e-1},\ g^{2e-1},\ g^{3e-1},\cdots g^{fe-1} \end{array}\right\} \qquad (15)$$

任何組內根之和, 名爲一"週期"。故各週期如下:

$$\eta_k=r^{g^k}+r^{g^{e+k}}+r^{g^{2e+k}}+\cdots+r^{g^{(f-1)e+k}},\ (k=0,1,\cdots e-1) \qquad (16)$$

設$f=e'\cdot f'$ 爲f之因子解法。則$p-1=ee'\cdot f'$。如前, 可得

$\eta_j' = r^{g^j} + r^{g^{ee'+j}} + r^{g^{2ee'+j}} + \cdots + r^{g^{(f'-1)ee'+j}}, (j = 0, 1, \cdots ee'-1)$ (17)

每週期(16)乃是某e'週期(17)之和，

$\eta_k = \eta'_k + \eta'_{e+k} + \eta'_{2e+k} + \cdots + \eta'_{(e'-1)e+k}, (k = 0, 1, \cdots e-1)$ (18)

而我們已知道此右端內有每一根 $r^{g^{se+k}}, (s = 0, 1, \cdots f'e'-1)$ 一次且祇一次，η_k 亦然。

設$f' = e''f''$爲f'之因子分解。則$p-1$爲$ee'e''$與f''之積，故

$\eta_t'' = r^{g^t} + r^{g^{ee'e''+t}} + r^{g^{2ee'e''+t}} + \cdots + r^{g^{(f''-1)ee'e''+t}}, (t = 0, 1, \cdots ee'e''-1)$ (19)

每週期(17)是某e''週期(19)之和，

$\eta'_j = \eta''_j + \eta''_{ee'+j} + \eta''_{2ee'+j} + \cdots + \eta''_{(e''-1)ee'+j}, (j = 0, 1, \cdots ee'-1)$ (20)

仿此，再可設$f'' = e'''f'''$，等等，直至$f^{(l)} = 1$爲止。如是，每週期分成爲項數較少的諸週期，最後的週期祇有一項。例如，$p = 17$，可取$e = 2$，$f = 8, e' = 2, f' = 4, e'' = 2, f'' = 2, e''' = 2, f''' = 1,$

而得19節內之週期。

下面二定理，38節內證之：

定理一 週期 $\eta_0,\ \eta_1,\ \cdots\eta_{e-1}$ 乃是一方程 $F(x)=0$ 其次數爲e係數爲整者之根。

定理二 e' 個週期，每個爲f' 項者：

$$\eta'_k,\ \eta'_{e+k},\ \eta'_{2e+k},\cdots\eta'_{(e'-1)e+k} \tag{21}$$

其和爲 η_k，乃是一方程 $\phi'_k(x)=0$ 之根，其次數爲e'，係數則爲 $\eta_0,\ \eta_1,\cdots\ \eta_{e-1}$ 之一次的函數(其係數爲整的)。

定理二所述於 $p-1$ 之任何因子解法均可用，故可稍改變其記號法，用於其他的因子解法上。我們可取因子ee'，e''，f''，卽知 e''個週期，每個 f'' 項者：

$$\eta''_k,\ \eta''_{ee'+k},\ \eta''_{2ee'+k},\ \cdots\eta''_{(e''-1)ee'+k} \tag{22}$$

其和爲 η'_k，乃是一方程$\phi''_k(x)=0$ 之根，其次數爲 e''，係數爲 $\eta'_0,\ \eta'_1,\cdots\eta'_{ee'-1}$ 之一次函數(係數爲整者)。又取 $ee'e''$，f'''，e'''，則可知 e''' 個週期，每個f''' 項者：

$$\eta'''_{k},\ \eta'''_{ee'e''+k},\ \eta'''_{2ee'e''+k},\ \cdots,\ \eta'''_{(e'''-1)ee'e''+k}$$

(23)

其和爲 η''_k，乃是一方程 $\phi'''_k(x)=0$ 之根，其次數爲 e'''，係數爲 $\eta''_0, \eta''_1, \cdots \eta''_{ee'e''-1}$ 之一次函數(係數爲整者)。最後，可得 $e^{(l)}$ 次的方程爲一項所成的週期所滿足。於是可知設 $e, e', \cdots e^{(l)}$ 爲整數，其積爲 $p-1$，則可決定一系方程

$$F(x)=0,\ \phi'_k(x)=0,\ \phi''_k(x)=0,\ \cdots\ \phi^{(l)}_k(x)=0, \qquad (24)$$

其次數爲 $e, e', e'', \cdots e^{(l)}$，者，此中第一個之係數是整的，而其餘各個之係數乃是(帶有整係數的)其前者之根之一次函數，而最後者之根，乃是 1 (10)之雜 p 次根。

22. 設 $p-1$ 爲2之乘方，則 $e, e', \cdots$ 可均爲2，俾 (24) 統爲二次方程。於應用至於有法多邊形上，可略去末後的方程，其根爲1之 p 次雜根者，因我們祇需要 $r+r^{-1}$，而 $r+r^{-1}$ 乃是(24)中一方程，適在其前者，之一根。欲證此，可注意由第

七篇47節p之質根 g 滿足 $g^e \equiv -1 \,(mod.\ p)$，這裏 $e=\frac{1}{2}(p-1)$，俾 $r^{g^r}=r^{-1}$。但欲得祇有二項的週期 η_k，則必使 $f=2, e=\frac{1}{2}(p-1)$ 於 (16) 內。於是 $\eta_k=r^{g^k}+r^{g^{e+k}}=r^{g^k}+r^{-g^k}$。由 16 節開首所說，$\eta_k$ 是實數。因所含項數多於2的週期爲恰含二者之和，故知每週期是一實數，除一項的週期不計。因知用以計算 $r+r^{-1}=2cos\frac{2\pi}{p}$ 的二次方程，一切均有實根。所以若$p-1$爲2^h形式，$2cos\frac{2\pi}{p}$之值可由解一組二次方程（有實根者）得之，照3節，$\frac{2\pi}{p}$可用界尺與圓規爲之。於是得此**定理**：

設p爲2^h+1式的質數，則可用界尺與圓規作一有法p邊形切入圓內。

23. 次論有法n邊形，於此n有二個或多個不同的因子 $p,q,\cdots$，卽$n=p^s\cdot q^t\cdots$

設如已得一n邊形，則可連某個頂點而得一p^s邊或q^t邊的形。反之亦然。廣之，設a與b互質，

則自a邊形與b邊形可推得一ab邊形。由第七篇32節，可有整數c與d，能$ca+db=1$者。因有$\frac{2\pi}{a}$與$\frac{2\pi}{b}$角，可作其倍角，幷加之，即得

$$d\cdot\frac{2\pi}{a}+c\cdot\frac{2\pi}{b}=\frac{2\pi}{ab}(db+ca)=\frac{2\pi}{ab},$$

因而可作有法ab邊形。於是證得此定理：

設$n=p^s q^t\cdots(p,q,\cdots$為不同的質數$)$，則當有法$p^s$邊，$q^t$邊，…形能切入圓內時，且祇當此時，纔能用界尺與圓規切入有法n邊形於圓內。

24. 今祇須再論一有法多邊形，其邊數乃是質數之乘方，如p^s。1之p^s次根為$x^{p^s}=1$之根，但非$x^{p^{s-1}}=1$之根，其形式作

$$r=\cos\frac{2\pi}{p^s}+i\sin\frac{2\pi}{p^s}$$

故r是以下方程之根：

$$\frac{x^{p^s}-1}{x^{p^{s-1}}-1}=x^{p^{s-1}(p-1)}+x^{p^{s-1}(p-2)}+\cdots+x^{p^{s-1}}+1=0 \qquad (26)$$

31節內將指出，此方程於有理數領域內不可化。

倘有法p^s邊形能用界尺與圓規切入圓內，則其各頂點之坐標 x_k，y_k 除實平方根外無其他無理性。故x_k+iy_k 除實或幻的平方根外，無其他無理性。前5−10節內所論，根數不限於實者。故照10節，(26)之次數必爲2之乘方。設$S>1$，則除$p=2$外，$p^{s-1}(p-1)$非爲2之乘方。故得 **定理**：設p爲質數>2，則如$S>1$，或$S=1$，以及$p-1$非爲2^h形式時，有法p^s邊形卽不能用界尺與圓規切入圓內。

25. 照此定理幷22節之定理，故知設p爲質數>2，則祇當p爲2^h+1形式時，有法p邊形乃可用界尺與圓規爲之。我們知道設 $h=(2k+1)q$，則2^h+1非質數，蓋如是2^h+1可有因子 2^q+1。如h無奇因子，則必爲2之乘方 2^t。於是得：

設p爲質數>2，則當p 爲以下形式時，且祇當此時，有法 p 邊形乃可用界尺與圓規作之：

$$2^{2^t}+1 \tag{27}$$

26. 於是引起此問題：t 爲何數時，(27) 是質數。於$t=0,1,2,3,4$，(27)爲 3,5,17,257,65537，

均爲質數。有名算術家梵馬 (*Fermat*) 曾猜想以爲 t 爲任何數，(27)均是質，但歐拉 (*Euler*) 證明 $t=5$，(27)即非質：

$$2^{32}+1=641\cdot 6700417。$$

又，於 $t=6,7,8,9,11,12,18,23,36,38,73$，(27)亦非質。

27. 因任何一角可平分之，故如有法k邊形可作，則$2k$邊形亦可作。於是得**定理**：

設$n=2^l p_1 p_2\cdots(p_1, p_2,\cdots$爲不同的作$2^{2^t}+1$形式的質數)，且祇是如此，$n$邊有法形乃可用界尺與圓規爲之。

最小的諸 p_i 是 3,5,17,257,65537。於$t=5,6,7,8,9$，此數非爲質。於$t=10$，此數有155位，至其是否爲質，則尚未定。

有法 n 邊形，$2<n<26$，可分爲二類：

可切入者：3,4,5,6,8,10,12,15,16,17,20,24；

不可切入者：7,9,11,13,14,18,19,21,22,23,25。

28. 1之質根 $x^n=1$之根r，倘不能滿足$x^l=1$，

於此 $0<l<n$，則名爲1之 n 次質根。例如 $i=\sqrt{-1}$ 乃是1之四次質根，因 $i^4=1$，而 i, i^2, i^3 與1不同。又如

$$r_1=\cos\frac{2\pi}{n}+i\sin\frac{2\pi}{n}$$

乃是1之n次質根；照德氏定理，$r_1{}^n$是 r_1 之至小正乘方等於1。

設r爲任何1之n次質根，則

$$r,\ r^2, \cdots, r^n \tag{28}$$

乃是1之一切n次根。事實上，這些乘方乃是$x^n=1$之根，各相不同的；而n次的方程，其根不能多於n個。

我們不難決定(28)中何者是1之n次質根。試論r^k，而設g爲k與n之最大公約數，則$(r^k)^{\frac{n}{g}}=(r^n)^{\frac{k}{g}}=1$。故設 $g>1$，而 $\frac{n}{g}<n$，r^k 非爲1之n次質根。但設$g=1$，則可有整數a與b存在（第七篇32節），能$ak+bn=1$者。

於是，設$(r^k)^l=1$，$0<l<n$，可得

$$r^l = r^{(ak+bn)l} = (r^{kl})^a (r^n)^{bl} = 1,$$

而 $r^l \neq 1$。故設 $g=1$，r^k 是質根。如是，已證明當 r 爲1之任何 n 次質根時，則祇當 k 與 n 互質，r^k 亦是質根。

例如 $i=\sqrt{-1}$ 乃是 1 之四次質根，$i^3=-i$ 亦然，而 $i^2=-1$ 非是。

前面定理又可如是述之：設 r 爲1之任何 n 次質根，而設 $1, a, b, \cdots l$ 爲整數統 $< n$ 與 n 互質，則

$$r,\ r^a,\ r^b, \cdots r^l \tag{29}$$

爲1之一切不同的 n 次質根。

29. 設 $n=p^s$，p 爲質數，而設 r 爲1之 p^s 次質根。$x^{p^s}=1$ 之 $n=p^s$ 個根(28)中，$r^p, r^{2p}, \cdots r^{p^s}$ 乃是 $x^{p^{s-1}}=1$ 之 p^{s-1} 個不同的根。其餘 p^s-p^{s-1} 個根乃是1之 p^s 次質根。故(26)之根乃是1之一切 p^s 次質根。

欲完成24節之討論，可證明此方程於一切有理數領域內不可化。此證基於一極重要的補題上。於特例 y^3-3y+1，此補題說明此函數乃是有理

係數的二因子之積，祇當這些係數是整數時纔如此。此則於12節內已證之。

30. 高斯之補題 設如一整函數$f(x)$，其係數爲整的，最高的乘方者是1，乃是二整函數之積：

$\phi(x)=x^m+b_1x^{m-1}+\cdots b_m$，$\psi(x)=x^{m'}+c_1x^{m'-1}+\cdots+c_{m'}$，(係數爲有理的)則這些係數是整數。

將分數$b_1,\cdots b_m$化成有最小公母β_0者，而設$b_i=\frac{\beta_i}{\beta_0}$。因之，$\beta_0,\cdots\beta_m$無公因子。仿此，可設$c_i=\frac{\gamma_i}{\gamma_0}$，而$\gamma_0,\cdots\gamma_{m'}$亦無公因子。用$\beta_0\gamma_0$乘$f=\phi\cdot\psi$，得

$$\beta_0\gamma_0 f(x)=\phi_1(x)\cdot\psi_1(x) \qquad (30)$$

於此，$\phi_1(x)=\beta_0x^m+\beta_1x^{m-1}+\cdots+\beta_m$，$\psi_1(x)=\gamma_0x^{m'}+\gamma_1x^{m'-1}+\cdots+\gamma_{m'}$。倘$\beta_0=\gamma_0=1$，則此補題已證明。今設$\beta_0\gamma_0>1$，則(30)左端之每項是$\beta_0\gamma_0$之質除數$p$之倍數。一切$\beta$不能均有公因子$p$。設$\beta_i$爲$\phi_1(x)$中第一係數，不能爲$p$除者。$\gamma$中亦至少有一個不能用$p$除者，今設$\gamma_k$爲其第一個。

$\phi_1(x)\cdot\psi_1(x)$ 中 $x^{m+m'-i-k}$ 之總係數是 $\beta_i\gamma_k+\beta_{i-1}\gamma_{k+1}+\beta_{i-2}\gamma_{k+2}+\cdots+\beta_{i+1}\gamma_{k-1}+\beta_{i+2}\gamma_{k-2}+\cdots$，此數必能爲 p 除，因(30)左端之每項均能爲 p 除。照所設，β_{i-1}，β_{i-2}，$\cdots$ 與 γ_{k-1}，γ_{k-2}，$\cdots$ 可爲 p 除，故 $\beta_i\gamma_i$ 亦必可除，此卽不合。

31. (26)不可化之證極多，今將克朗納格(*Kronecker*)之第一證重錄出。欲證明用(26)定下的函數 $f(x)$ 於有理數領域內不可化，祇須指出 $f(x)$ 不是二整係數的多項式 $\phi(x)$ 與 $\psi(x)$ 之積便行。今設 $f(x)$ 可解爲因子 $f(x)=\phi(x)\cdot\psi(x)$。於 $x=1$，得 $p=\phi(1)\cdot\psi(1)$。因 p 爲質數，其一整數如 $\phi(1)$ 必爲 ±1。設 r 爲1之 p^s 次質根。一切質根都已見於(29)，於此 $1,a,b,\cdots l$ 表出 $t=p^s-p^{s-1}$ 整數 $<p^s$ 與 p^s 互質者。由29節，(29)乃是(26)之一切根。故 $\phi(x)$ 於其中一數代入 x 時必成0，而

$$\phi(r)\cdot\phi(r^a)\cdot\phi(r^b)\cdots\phi(r^l)=0。$$

換言之，將任何 p^s 次質根 r 代入 x 時，函數

$$P(x)=\phi(x)\cdot\phi(x^a)\cdot\phi(x^b)\cdots\phi(x^l)$$

成0。因$P(x)$於$f(x)$之每一根均成0，而$f(x)$之根均不同，故$P(x)$可爲$f(x)$所除。如是，$P(x)=f(x)\cdot q(x)$[$q(x)$爲整係數的多項式]。$P(x)$中ϕ之數是t，故於$x=1$，

$$[\phi(1)]^t=p\cdot q(1)。$$

因$\phi(1)=\pm 1$，p不能除$[\phi(1)]^t$。故假定$f(x)$可化卽不合。

32. 21節內定理之證，建立於四補題上，今具述之。

21節內用r表1之一個p次根$\cos\frac{2\pi}{p}+i\sin\frac{2\pi}{p}$，這裏則用以表任何一$p$次的1之質根。由28節，(9)爲1之一切雜$p$次根；(10)亦然。故若$r$爲1之任何一質根$p$次者，則(10)可恰如21節之分成爲週期。

33. 初等代數學內曾指出，設如一方程$F(x)=0$(係數爲實者)有一雜根$a+ib$($i=\sqrt{-1}$，$b\neq 0$)，則并有$a-ib$爲根，而$F(x)$有因子$\phi(x)=(x-a-ib)(x-a+ib)=x^2-2ax+a^2+b^2$。因$\phi(x)$無因子$x-d$($d$爲實數)，故於實數領域內不可化。

而此卽是下面補題之特例：

補題I 設$F(x)$與$\phi(x)$爲整函數，係數在D，而$\phi(x)$在D內不可化，則若$F(x)$於$\phi(x)=0$之一根x_1成0，$F(x)$卽是$\phi(x)$與一係數在D內的整函數之積。

尋常求$F(x)$與$\phi(x)$之最大公因子$g(x)$祇須用有理算法便行，故$g(x)$之係數在D內。又，$g(x)$非爲常數，因$F(x)$與$\phi(x)$有公因子$x-x_1$。因$\phi(x)$於D內不可化，其因子$g(x)$必等於$c\phi(x)$，c爲常數。故$\phi(x)$與$g(x)$爲$F(x)$之因子。

系 設$F(x)$之次數$<\phi(x)$者，則$F(x)$之係數均爲0。

34. **補題II** 1之p次質根r之整函數$f(r)$可使之成正則式

$$c_0r+c_1r^g+c_2r^{g^2}+\cdots+c_{p-2}r^{g^{p-2}},\qquad(31)$$

於中c_i爲$f(x)$之係數之整函數（係數亦整）。設$f(r)$之係數爲有理的，則祇有一種正則式。

因$r^p=1$，$r\neq1$，r是

$$\frac{x^p-1}{x-1}=x^{p-1}+x^{p-2}+\cdots+x+1=0 \qquad (32)$$

之根。故 $$r^{p-1}+r^{p-2}+\cdots+r+1=0 \qquad (33)$$

用$r^p=1$，可使$f(r)$作此形式：

$$f(r)=a_0+a_1r+a_2r^2+\cdots+a_{p-1}r^{p-1}。$$

用a_0乘(33)由此減去，卽得

$$f(r)=A_1r+A_2r^2+\cdots+A_{r-1}r^{p-1} \qquad (34)$$

於此$A_i=a_i-a_0$。因(9)以某次序與(10)相同，故可使 (34) 作正則式 (31)。補題之第一段於是已證明。

今再假定起初的函數$f(r)$之係數是有理數。於是 a_i 與 A_i 均爲有理數。如是，則$f(r)$ 祇能作一種形式(34)表之。蓋若

$$f(r)=B_1r+B_2r^2+\cdots+B_{p-1}r^{p-1}$$

亦是一式，B_i 爲有理數，則相減幷剔去r後，得

$$0=A_1-B_1+(A_2-B_2)r+\cdots+$$
$$(A_{p-1}-B_{p-1})r^{p-2},$$

係數爲有理數。但(32)於有理數領域內不可化，故由前節之系，每一係數A_i-B_i爲0。

35. 週期(16)有此重要屬性，倘 r 易以 r^{g^e} 時均無變動。如是則 r^{g^s} 可易為 $(r^{g^e})^{g^s}=r^{g^{e+s}}$，俾一週期 η_k 之任何一項可用其次項易之，末項則用首項易之，蓋

$$g^{fe}=g^{p-1}\equiv 1\,(mod.\ p)。$$

36. 補題III 1之 p 次質根之任何整函數 $f(r)$，其係數 a_i 為整的，幷有此屬性，倘 r 易以 r^{g^e} 時，可仍不變者，等於一週期之一次函數：

$$k_0\eta_0+k_1\eta_1+\cdots+k_{e-1}\eta_{e-1} \qquad (35)$$

於此 k_i 為 a_i 之函數，有整的係數。設 a_i 均為整數，則 k_i 為整數。

將 $f(r)$ 作正則式(31)，但 r 之乘方列之為(15)式：

$$f(r)=c_{00}r+c_{10}r^{g^e}+c_{20}r^{g^{2e}}+\cdots+c_{f-1\,0}r^{g^{(f-1)e}}$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$+c_{0k}r^{g^k}+c_{1k}r^{g^{e+k}}+c_{2k}r^{g^{2e+k}}+\cdots\cdots\cdots\cdots$$

$$+c_{f-1\,k}r^{g^{(f-1)e+k}}$$

將 r 易以 r^{g^e}，則任何列之乘方均轉輾變互。所得

函數之係數必等於$f(r)$者，故

$$c_{0k}=c_{1k},c_{1k}=c_{2k},\cdots,c_{f-1k}=c_{0k},$$

$$(k=0,1,\cdots e-1)。$$

如是，每列中之諸c皆等。剔去公因子，卽得r諸乘方之和，定一週期η_k。故$f(r)=c_{00}\eta_0+c_{01}\eta_1+\cdots+c_{0k}\eta_k+\cdots+c_{0e-1}\eta_{e-1}$。

37．補題IV 1之p次質根之整函數$f(r)$，其係數爲整的，而將r易以r^g時不變者，等於一整數。

用補題III於$e=1$，則$\eta_0=r+r^g+r^{g^2}+\cdots+r^{g^{p-2}}$爲僅有的週期。由(33)，$\eta_0=-1$；故由(35)$f(r)=-k_0$。

38．今乃可證21之定理一與二。第一，$\eta_0,\cdots\eta_{e-1}$乃是

$$F(x)=(x-\eta_0)(x-\eta_1)\cdots(x-\eta_{e-1})=0$$

之根。其係數爲η_i之相稱函數，係數爲整的。將r易以r^g，這些週期卽輾轉變互，卽是，η_0易爲η_1，η_1易爲η_2，等等。故其相稱函數不變動，而照補

題IV，等於一整數。定理一即已明白。

其次，週期(21)乃是

$$\phi'_k(x)=(x-\eta'_k)(x-\eta'_{e+k})\cdots(x-\eta'_{(e'-1)e+k})=0$$

之根，其係數乃是(21)之相稱函數(係數爲整)。若r易以r^{g^e}時，後者即輾轉變互。故由補題III即得定理二。

圓周率π之歷史及其超絕性

David Eugene Smith著

目　次

圓周率π之歷史及其超絕性

David Eugene Smith 著

1.　問題之性質　人類最初準確測量得的面積，自然是直角方形，尤是正方形，無疑。倘直角方形之邊有度量上的公單位可通約之，則此問題不難解決了；而實用上，亦總可找得此。其第二步或者是測量平行方形或三角形，後此則繼之以梯形，最普通的直線形於是完了。理論上，這些多邊形之測量向不大難，而由此則其他多邊形之面積亦已可求得。及至求曲線形之面積，即有

困難了，其最普通者，古時已早有此項努力，想求得一與已知圓等積的正方形，然後由此計算圓之面積。換言之，卽是"求圓之方"的問題。倘若能求得一與圓周等長的直線，則此問題卽可解決；於是此問題成爲"求圓周之直線"的問題了。而倘若我們能求得圓周率 π 之値爲一整數或分數或小數，則此問題又不難解決；又因可用界尺與圓規作某種圖形故，所以若能以有限數的平方根表 π，換言之，若能用有理算法及祇有一定數的平方根之無理算法表出 π，則此問題亦卽可解。反之，凡用界尺與圓規爲之的幾何作法，無異於決定二直線之相交，一線與一圓之相交，或二圓之交，等於有理算法或開平方。故凡不如是者，卽不可作(參觀第八篇2,11兩節)。於是此問題成爲決定 π 之性質的問題，卽 π 是否爲一代數方程之根，可如是得之者。

2、 此問題之歷史 此問題之歷史可分爲三時代論之。第一時代自古時至十七世紀之中；此時

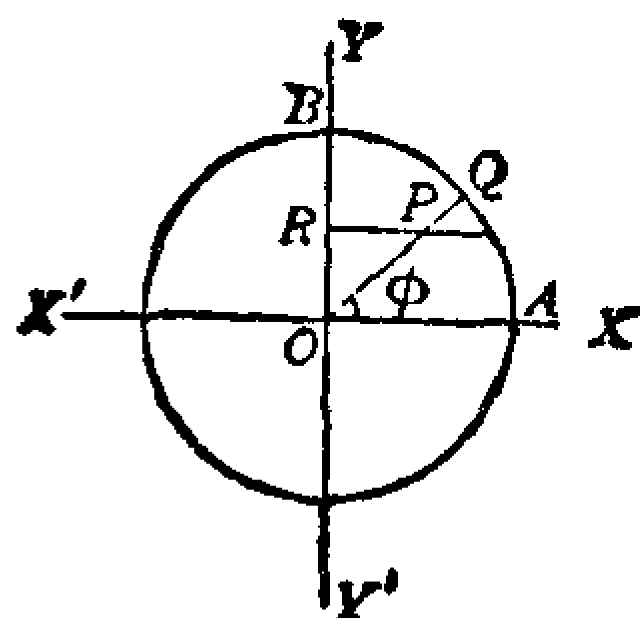
代中大都是求一正方等於一已知的圓者等努力，或用目前的初等教科書中所述的那種純粹幾何方法，求 π 之近似値。第二時代約有一百年之久，自發明微積分起至1766年良伯 (*Lambert*) 發表關於此的著作止。此時代中之特色，乃是解析方法代了古時的幾何方法，研究者中之尤著名的，有牛頓，萊伯尼玆 (*Leibnitz*)，柏諾利兩昆仲 (*Bernoulli*)，歐拉 (*Euler*) 等諸人。這時代中，不用古時的“竭盡法”，而用無限級數及乘積以求 π 之値，有歐氏公式等。第三時代則自十八世紀之中起直至今日；其特色在求 π 之性質，是否爲有理的，抑係代數的或超絕的。所謂“代數數目”者，乃是能爲方程 $C_0+C_1x+C_2x^2+\cdots+C_nx^n=0$ (C_0, C_1,$\cdots C_n$ 爲有理數)之根的數目；不則稱爲“超絕數目”。又，倘一數目是一代數方程帶有理係數者之根，則必亦爲帶整係數者之根。爲此，我們可限於整係數的方程。

第一時代之開始，已在有史以前，聖經上載 π

之值爲3,上古時大都如是。巴比倫(*Babylonian*)人對此的見解,迄今未有所知,而古印度人及中國人之上古紀載,則不可靠。但在埃及人方面,則曾發見四千年前的π之值爲$\frac{256}{81}$或3.1604……。

古希臘哲學家中,曾有不少的人想解決此問題。最初對此有供獻的,爲伊里之希璧亞司(*Hippias of Elis*)(紀元前四百餘年),他發見一曲線,即所謂"求直曲線"(*quadratrix*)者是。此曲線尋常稱爲地諾司德拉圖(*Dinostratus*)氏之曲線,蓋他曾詳細研究過此。

此曲線可述之如下:以直角坐標系之起點爲心作單位圓,設Q與R爲二點,以整齊的速度一於AB弧上一於OB半徑上運動,由A與O同時起,



并同時至B，則OQ與R點OB之垂線之相交點P作出一求直曲線。這裏，縱坐標y與角ϕ爲比例的。當$y=1$時，$\phi=\frac{\pi}{2}$，故$\phi=\frac{\pi}{2}\cdot y$。又因

$\phi=arc\ tan\ \frac{y}{x}$，故$\frac{y}{x}=tan\frac{\pi}{2}\cdot y$，而

$x=\frac{y}{tan\frac{\pi}{2}y}$。因之，此曲線遇$x$軸於

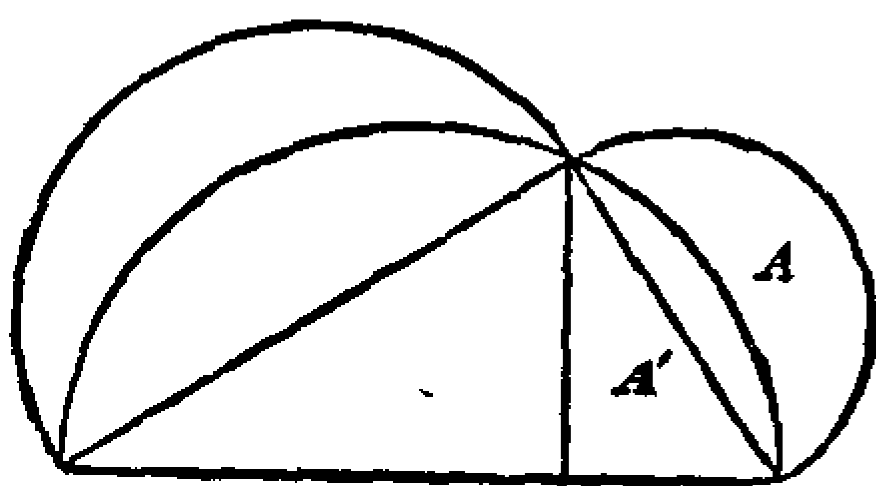
$$x=\lim_{y=0}\frac{y}{tan\frac{\pi}{2}y}=\frac{2}{\pi}。$$

倘我們能作出此曲線，則卽能得此值，因而不難由此以推π。然作此曲線之困難，則與求π同，實際上乃是相同的問題。

與希氏同時者，有安抵風(*Antiphon*)與柏拉孫(*Bryson*)兩人，目前解初等幾何學上問題的方法，他們多所供獻。安氏用內切多邊形增加邊數之法，以求圓面積之近似値。柏氏則於內切形外，并作相似的外切形，而以爲圓之面積，乃是前二者之算術的平均値，所設雖不合，但又逼近了一

步。安氏方法，實已開近代微積算法之先聲。

想求圓之方的第一人，是喜帕克拉底（*Hippocrates*，紀元前 450 年）。他證明倘於直角三角形之各邊上如圖所示作半圓，則月形 A 等於三角形 A'，此法於圓之普通問題上實無所供獻。



希臘人中之最有供獻者，爲亞幾默德（*Archimedes*），他有量圓法之命題三條。實際上，他的方法仍是增加內外切形邊數之法，以倍數進行，與今日初等幾何學中者同。用此法，他求得 $3\frac{1}{7}>\pi>3\frac{10}{71}$，故 $3\frac{1}{7}$ 亦稱亞氏率，而因其便於計算，至今仍還用之。其後托來末（*Ptolemy*）改良亞氏率，得 $\pi=3.14166\cdots\cdots$。

在印度人方面，約當紀元後五百年時，其率亦與此相似；亞拉巴太（*Aryabhatta*）曾設 $\pi=3$，

1416。稍後，則有婆羅馬古太(*Brahmagupta*)，所得值與亞氏率同。當中世紀時，此率使用極廣。

在中國人方面，於此頗有可注意的獲得。東漢安帝時人張衡(西曆78-139年)曾得$\pi=\sqrt{10}$。後此，則當三國時吳人王蕃(西曆229-267年)求得$\pi=142:45$或3.1555…，而同時劉徽用一種方法與安抵風法相同者，獲3.14。最可注意的，則爲宋末南齊祖沖之(約當西曆四百餘年時)的發見，他求得π之值在3.1415926與3.1415927之間，幷知$\frac{22}{7}$與$\frac{355}{113}$乃是其近似值。後者尋常稱爲安托尼玆(*Adriaen Anthonisz*，十六七世紀時人)率，實則祖氏早已發見了。其後還有人計算此值，惟未有良好結果。清初康熙時(十八世紀之初)所編"數理精蘊"上載π之值至十九位。

歐洲當中世紀時，皮舍諾(*Pisano*)求得$\pi=3.1418$。自後直至十七世紀時，始有安托尼玆重發見中國祖沖之在千餘年前所早已知道的值$\frac{355}{113}$。同時有維太(*Viète*)用希臘人的方法，取$6\cdot2^{16}$邊

形，求得π之值與今時所用有九位相同。而羅曼(*A. Romanus*, 亦當此時)則計算π之值至十七位小數。稍後，即有魯道爾夫(*Ludolph*)推廣至三十五位，因此，至今德國方面有稱π爲魯氏數者。最後，胡耕詩(*Huygens*)用此項方法，祇取60邊形，而得九位之數。第一時代於是告終了。

第二時代以十七世紀後半紀爲始，已有新的解析方法供應用，牛頓，萊伯尼玆，梵馬(*Fermat*)，華里士(*Wallis*)，白朗克(*Brouncker*)，伯諾利昆仲等於是大有供獻。古時的幾何方法到此不用了，其所用者性質上與前此的根本不同，乃是解析的表出π，展之爲無限級數或乘積。此中首爲華里士之工作，他證明

$$\frac{\pi}{2}=\frac{2}{1}\cdot\frac{2}{3}\cdot\frac{4}{3}\cdot\frac{4}{5}\cdot\frac{6}{5}\cdot\frac{6}{7}\cdot\frac{8}{7}\cdot\frac{8}{9}\cdots$$

以及

$$\frac{4}{\pi}=1+\cfrac{1}{2+\cfrac{9}{2+\cfrac{25}{2+\cfrac{49}{2+\cfrac{81}{2+\cdots}}}}},$$

此第二連分式，實則白朗克已得之，惟無證。

此時所得最重要的無限級數用以計算圓者，是格里郭(*J. Gregory*)於1670年及萊伯尼茲於1673年所發見的級數：

$$arc\ tan\ x = x - \frac{x^3}{3} + \frac{x^5}{5} - \frac{x^7}{7} + \cdots$$

格氏曾知須研究此級數之收斂性，萊氏則稍後從事之。格氏并曾說過，普通圓之扇形與其內切或外切形之面積之比不能用有限數的代數項表出之。

$arc\ tan\ x$ 之級數中倘$x=1$，卽得

$$\frac{\pi}{4} = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \cdots$$

然此級數收斂極慢，實用上頗不便。通常此級數稱爲萊氏級數，實則非彼一人所發見。倘於此級數中不設$x=1$，而設$x=\sqrt{\frac{1}{3}}$，則得

$$\frac{\pi}{6} = \sqrt{\frac{1}{3}} \cdot \left(1 - \frac{1}{3\cdot3} + \frac{1}{3^2\cdot5} - \frac{1}{3^3\cdot7} + \frac{1}{3^4\cdot9} - \cdots\right),$$

此較前者爲便於用。若更用反三角函數上之定理加以變化，則可得更便利者：$\frac{\pi}{4}=4\ arc\ tan\frac{1}{5}-arc\ tan\frac{1}{239}$

$$=4\left(\frac{1}{5}-\frac{1}{3\cdot5^3}+\frac{1}{5\cdot5^5}-\frac{1}{7\cdot5^7}+\cdots\right)$$

$$-\left(\frac{1}{239}-\frac{1}{3\cdot239^3}+\frac{1}{5\cdot239^5}-\cdots\right),$$

此式爲梅卿(*Machin*)所得，用之可計算π之値至100位。

此外，略可一述者，有拉格尼（*Laguy*）氏計算π至127位小數；范箈(*Vega*)至140位，大才(*Dase*)至200位，黎希德（*Richter*）至500位小數，山克(*Shanks*)至700位。由此，可見此項解析方法之遠勝於古法，不過實用上則自不必如此。但關於π之性質，究竟這是一有理數或無理數，抑或其他，則尙未能由此窺得。

解決此π之性質的問題，歐拉實於其關於訥氏對數底e的公式建下基礎。試自麥老令(*MacLaurin*)公式

$$f(x)=f(0)+f'(0)x+f''(0)\frac{x^2}{2!}+f'''(0)\frac{x^3}{3!}+\cdots$$

入手，可知　$e^x=1+x+\frac{x^2}{2!}+\frac{x^3}{3!}+\cdots,$

$$\cos x=1-\frac{x^2}{2!}+\frac{x^4}{4!}-\cdots,$$

$$\sin x=x-\frac{x^3}{3!}+\frac{x^5}{5!}-\cdots,$$

均是收斂的。由此，歐拉證明

$$e^{ix}=1+ix-\frac{x^2}{2!}-\frac{ix^3}{3!}+\cdots$$

以及　$i\sin x=ix-\frac{ix^3}{3!}+\frac{ix^5}{5!}-\cdots,$

故　$e^{ix}=\cos x+i\sin x$。

設$x=\pi$，卽得　$e^{i\pi}=-1$，或 $1+e^{i\pi}=0$，

此式內所含五個數，盡是數學上最可注意者。歐氏得此式後約百有五十年，始藉其助以證明 π 之超絕性。

歐氏還作出其他 π 與 e 之關係，以及用無限級數及乘積與連分各樣的表出此二者之值。例如：

$$\frac{\pi^2}{8}=1+\frac{1}{3^2}+\frac{1}{5^2}+\frac{1}{7^2}+\cdots,$$

$$\frac{\pi^3}{32}=1-\frac{1}{3^3}+\frac{1}{5^3}-\frac{1}{7^3}+\frac{1}{9^3}-\cdots,$$

$$\frac{\pi^2}{6}=\frac{2^2}{2^2-1}\cdot\frac{3^2}{3^2-1}\cdot\frac{5^2}{5^2-1}\cdot\frac{7^2}{7^2-1}\cdot\frac{11^2}{11^2-1}\cdots,$$

$$e=2+\cfrac{1}{1+\cfrac{1}{2+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{4+\cfrac{1}{1+\cdots}}}}}},$$

$$\frac{e-1}{2}=\cfrac{1}{1+\cfrac{1}{6+\cfrac{1}{10+\cfrac{1}{14+\cfrac{1}{18+\cdots}}}}}。$$

第三時代以良伯之著作爲始。他於關於此的著作中有二根本命題：

(1) 設 x 爲有理數非爲 0 者，則 e^x 不能爲有理的；

(2) 設 e^x 爲有理的，非 0，則 x 不能爲有理的。

他自歐拉之 $\frac{e-1}{2}$ 的公式（見前）入手，而指出

$$\frac{e^x-1}{e^x+1}=\cfrac{1}{\cfrac{2}{x}+\cfrac{1}{\cfrac{6}{x}+\cfrac{1}{\cfrac{10}{x}+\cfrac{1}{\cfrac{14}{x}+\cdots}}}}$$

以及 $\tan x=\cfrac{1}{\cfrac{1}{x}-\cfrac{1}{\cfrac{3}{x}-\cfrac{1}{\cfrac{5}{x}-\cfrac{1}{\cfrac{7}{x}-\cfrac{1}{\cfrac{9}{x}-\cdots}}}}}$,

由此項連分，他卽得如是的結論，其證實不嚴格。於 $x=\frac{\pi}{4}$，我們得 $\tan\frac{\pi}{4}=1$，故他說 π 不能爲有理的。良氏之誤，後經萊根德(*Legendre*)爲之訂正。故 π 之無理性，實由萊氏始證明之，他幷曾證得 π^2 之無理性。

其次有廖維萊(*Lionville*)在1840年證明 e 不能爲有理係數的二次方程之根，卽，設 a,b,c 是有理的，則此方程 $ae^2+be+c=0$ 不可能。此實爲證實萊氏說之第一步，卽 π 或者非爲一代數數目，不能滿足有理係數的代數方程。於是問題分爲二重：倘有代數方程，則何種項數有限係數有理者

能爲 e 與 π 所滿足？有無此項不能滿足如是方程的數目？對此第二重萊氏已疑及之，而廖氏則於1844年證明確有不能滿足前述的代數方程的數目，故可分數目爲代數的與超絕的二類。

1873年時，赫米脫 (*Hermite*) 研究指數函數之結果，證明 e 是超絕數，其後卽有林德曼 (*Lindemann*) 根據赫氏之工作，證明 π 亦是超絕的。林氏之證，在於指出方程 $a_0+a_1e^p+a_2e^q+a_3e^r+\cdots=0$ 內，指數與係數不能均爲代數數目。歐氏方程 $1+e^{i\pi}=0$ 內係數旣爲代數的，故指數 $i\pi$ 不能爲代數的，因而 π 是超絕數。今將先證 e 之超絕性，然後再論 π。

3. e之超絕性 自赫氏證明 e 之超絕性後，繼起者頗不乏人，類多將此問題約成簡單了；對此有供獻者爲希爾白 (*Hilbert*)，霍爾維玆 (*Hurwitz*)，戈登 (*Gordan*) 等諸人。今錄一簡單證法如下：

欲證明 e 爲超絕的，須指出不能有此項普通方

程

$$C_0+C_1e+C_2e^2+\cdots+C_ne^n=0 \tag{1}$$

存在，於此n爲正整數，$C_0, C_1, \cdots$爲有理數，0亦在內，惟 C_0 與 C_n 假定其非 0，不則次數卽變動了。爲簡單計，今不用此項普通 n 次的方程，而用三次者，卽指出不能有方程

$$C_0+C_1e+C_2e^2+C_3e^3=0 \tag{2}$$

此項證法，實質上無異於普通 n 次者，然卻可簡便些，亦易廣之至普通方程。我們可先一論二重要函數，因使用多，表之爲 $f(x)$ 與 $F(x)$。$f(x)$ 爲有理整函數 n 次者，而 $f(0)=0$，其形式作

$$f(x)=a_1x+a_2x^2+a_3x^3+\cdots+a_nx^n,$$

[illegible] a_i 爲有理數。此證，在於選出一函數

$$f(x)=\frac{x^{p-1}[(x-1)(x-2)(x-3)]^p}{(p-1)!},$$

此中 p 爲質數，後當定之。設

$$f(x)=\frac{x^{p-1}[(x-1)(x-2)(x-3)]^p}{(p-1)!}=a_1x+a_2x^2+a_3x^3+\cdots+a_nx^n \tag{3}$$

則可知 $n=3p+p-1$，而 a_{p-1} 爲非是 0 的第一係數，因 x 之最低乘方是 x^{p-1}。若廣之，則可使其分子爲 $x^{p-1}[(x-1)(x-2)\cdots(x-m)]^p$，但於此前者已够用。

至其他一函數，則如下：

$$F(x)=f'(x)+f''(x)+f'''(x)+\cdots+f^{(n)}(x) \quad (4)$$

於此 $f'(x),\cdots f^{(n)}(x)$ 爲 $f(x)$ 之各次引生。今先述三補題，而其證則俟後面：

補題 I 設 $f(x)=a_1x+a_2x^2+\cdots+a_nx^n$，而設 S_n 爲 e^x 級數之首 n 項之和，$S_1=1$，$S_2=1+\frac{x}{1!}$，$S_3=1+\frac{x}{1!}+\frac{x^2}{2!}$，…

則由 (4) $$F(x)=1!S_1a_1+2!S_2a_2+3!S_3a_3+\cdots+n!S_na_n \quad (5)$$

而 $$F(0)=1!a_1+2!a_2+3!a_3+\cdots+n!a_n \quad (6)$$

補題 II 設 p 爲質數，n 爲正整數，C_0, C_1, C_2, C_3，爲整數，

則 $$C_0F(0)+C_1F(1)+C_2F(2)+C_3F(3)=$$

$$C_0(3!)^p+pQ \tag{7}$$

於此 Q 爲整數爲諸 C 及 p 所決定。

補題 III 設 $A_1=|a_1|, A_2=|a_2|, \cdots A_n=|a_n|$，而 $X=|x|$，

則 $$A_1X+A_2X^2+A_3X^3+\cdots+A_nX^n=$$

$$\frac{X^{p-1}[(X+1)(X+2)(X+3)]^p}{(p-1)!} \tag{8}$$

入手時先寫出於x任何值均收斂的級數以定e^x:

$$e^x=1+x+\frac{x^2}{2!}+\frac{x^3}{3!}+\cdots+\frac{x^n}{n!}+\cdots \tag{9}$$

并仍照補題 I 中以 S_n 表此級數之首 n 項之和。又可設

$$U_n=x^n+\frac{x^{n+1}}{n+1}+\frac{x^{n+2}}{(n+1)(n+2)}+\cdots \tag{10}$$

如 $U_1=x+\frac{x^2}{2}+\frac{x^3}{2\cdot3}+\cdots$, $U_2=x^2+\frac{x^3}{3}+\frac{x^4}{3\cdot4}+\cdots$ 等等，而用 $1!, 2!, 3!, \cdots, n!$ 繼次乘(9)，

則得

$$\left.\begin{aligned}
&1!\,e^x = 1!\,S_1 + x + \frac{x^2}{2} + \frac{x^3}{2\cdot3} + \cdots = 1!\,S_1 + U_1,\\
&2!\,e^x = 2!\,S_2 + x^2 + \frac{x^3}{3} + \frac{x^4}{3\cdot4} + \cdots = 2!\,S_2 + U_2,\\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
&n!\,e^x = n!\,S_n + x^n + \frac{x^{n+1}}{n+1} + \frac{x^{n+2}}{(n+1)(n+2)} + \cdots\\
&= n!\,S_n + U_n。
\end{aligned}\right\}(11)$$

用(3)之諸係數 $a_1, a_2, \cdots a_n$ 乘(11)，幷相加之，

卽得

$$(1!\,a_1 + 2!\,a_2 + \cdots + n!\,a_n)\,e^x = (1!\,S_1a_1 + 2!\,S_2a_2 + \cdots + n!\,S_na_n) + (a_1U_1 + a_2U_2 + \cdots)$$

由(6)知　$F(0) = 1!\,a_1 + 2!\,a_2 + \cdots + n!\,a_n$，

由(5)　$F(x) = 1!\,S_1a_1 + 2!\,S_2a_2 + \cdots + n!\,S_na_n$。

故卽得　$F(0)\,e^x = F(x) + a_1U_1 + a_2U_2 + \cdots + a_nU_n$。

爲便利計，設 $\psi(x) = a_1U_1 + \cdots + a_nU_n$　　(12)

於是有　$F(0)\,e^x = F(x) + \psi(x)$　　(13)

因之，我們得一 e^x 之式，與 $F(x)$ 或卽與(3)中之 p 相關。

試於(13)內 x 處相繼以 0,1,2,3 代入，用 C_0, C_1, C_2, C_3 乘之，卽：

$$\left.\begin{aligned} F(0)C_0 &= C_0F(0)+C_0\psi(0)\\ F(0)C_1e &= C_1F(1)+C_1\psi(1)\\ F(0)C_2e^2 &= C_2F(2)+C_2\psi(2)\\ F(0)C_3e^3 &= C_3F(3)+C_2\psi(3)\end{aligned}\right\}(14)$$

加之得 $F(0)[C_0+C_1e+C_2e^2+C_3e^3]=$

$$C_0F(0)+C_1F(1)+C_2F(2)+C_3F(3)+C_0\psi(0)+C_1\psi(1)+C_2\psi(2)+C_3\psi(3) \qquad (15)$$

我們的目的，是欲證明 $C_0+C_1e+C_2e^2+C_3e^3=0$ 之不可能，故若指出(15)之不可能，卽明白了。由(7)，若(15)可能，卽(2)可能，則得

$$0=[C_0(3!)^p+pQ]+[C_0\psi(0)+C_1\psi(1)+C_2\psi(2)+C_3\psi(3)] \qquad (16)$$

故現在的問題，是在證明(16)之不可能。欲證此，須證明

(1) $C_0(3!)^p+pQ$ 之絕對值大於或等於1；以及

(2) $C_0\psi(0)+\cdots+C_3\psi(3)$ 之絕對值小於1。

蓋如是則可得 $\pm 1 \pm n = 0 (n<1)$，因而(16)不可能。

(1)設p爲質數>3，非 C_0 之因子，則 $C_0(3!)^p$ 不能爲 p 所除，pQ 則可爲 p 除。因 C_0 非 0，故其絕對值 ≧1。

(2)我們知道諸數之和之絕對值，小於或至多等於諸數之絕對值之和；例如 $|2-2+2-2|=0$，而 $|2|+|-2|+|-2|+|2|=8$。而諸 ψ 則爲(10)中之 U 所定。由(10)

$$U_n=x^n\left[1+\frac{x}{n+1}+\frac{x^2}{(n+1)(n+2)}+\cdots\right]$$

如(8)那樣，設 $|x|=X$，得

$$|U_n|\leqq X^n\left[1+\frac{X}{n+1}+\frac{X^2}{(n+1)(n+2)}+\cdots\right]$$

而 $$|U_n|<X^n\left[1+\frac{X}{1!}+\frac{X^2}{2!}+\cdots\right]$$

因後者之分母均小了。由(9)

$$|U_n|<X^n e^x \qquad (17)$$

仿此，設 $|a_1|=A_1$，等等，卽得

$$|\psi(x)|<A_1|U_1|+A_2|U_2|+\cdots+A_n|U_n|。$$

照(17)，並使n繼次爲1,2,…，卽得

$$|\psi(x)|<e^x[A_1X+A_2X^2+\cdots+A_nX^n]$$

由(8) $|\psi(x)|<e^x\dfrac{X^{p-1}[(X+1)(X+2)(X+3)]^p}{(p-1)!}$，

故 $|\psi(x)|<e^x(X+1)(X+2)(X+3)$

$$\frac{[X(X+1)(X+2)(X+3)]^{p-1}}{(p-1)!} \qquad (18)$$

對於 X 之任何值，可取極大的 p 俾

$\dfrac{[X(X+1)(X+2)(X+3)]^{p-1}}{(p-1)!}$ 成爲任何隨意的小，故 p 充分大時 $|\psi(0)|$，$|\psi(1)|$，$|\psi(2)|$，$|\psi(3)|$ 均可隨意使之小。因之，$C_0\psi(0)+C_1\psi(1)+C_2\psi(2)+C_3\psi(3)$ 之絕對值，必可使其小於1。

如是，可知(16)不可能，(15)不可能，卽(2)不可能，而 e 非整係數的三次方程之根。此項結

果，因證內未嘗限 $n=3$，故可推至於 n 次的任何方程。於是證明了 e 之超絕性。

補題 I 之證　我們可寫 $f(x)$ 作此式：

$$f(x)=1!a_1\frac{x}{1!}+2!a_2\frac{x^2}{2!}+\cdots+n!a_n\frac{x^n}{n!}。$$

則 $f'(x)=1!a_1+2!a_2\frac{x}{1!}+3!a_3\frac{x^2}{2!}+\cdots+n!a_n\frac{x^{n-1}}{(n-1)!}$

$$f''(x)=\qquad 2!a_2 \quad +3!a_3\frac{x}{1!}+\cdots+n!a_n\frac{x^{n-2}}{(n-2)!}$$

....

$$f^{(n)}(x)=\qquad\qquad\qquad\qquad n!a_n$$

加之，卽得

$$f'(x)+f''(x)+\cdots+f^{(n)}(x)=1!S_1a_1+\cdots+n!S_na_n。$$

補題 II 之證　將 $f(x)$ 寫作

$$f(x)=\frac{B_{p-1}x^{p-1}+B_px^p+\cdots+B_{4p-1}x^{4p-1}}{(p-1)!},$$

這裏諸 B 均爲整數，因是整數之積，而

$$B_{p-1}=[(-1)(-2)(-3)]^p=\pm(3!)^p。$$

取其各次引生，而設 x 爲 0，則得

$$f'(0)=0,\ f''(0)=0,\cdots f^{(p-2)}(0)=0,$$

而 $f^{(p-1)}(0)=B_{p-1}$，$f^{(p)}(0)=pB_p$，$\cdots f^{(n)}(0)=p(p+1)\cdots nB_n$。

故　$F(0)=B_{p-1}+pB_p+\cdots+[p(p+1)\cdots nB_n]$。

將前 B_{p-1} 之值代入，得 $C_0F(0)=C_0(3!)^p+$ 許多有 p 爲因子的整數。

仿此，可知 $F(1),F(2),F(3)$ 均等於有 p 爲因子的一組整數。相加後，卽得(7)。

補題 *III* 之證　由

$$f(x)=\frac{x^{p-1}[(x-1)(x-2)(x-3)]^p}{(p-1)!}，可知$$

$f(x)$ 各項之號正負相雜，故改爲正號時乃能相等得(8)。

4. π 之超絕性　π 之超絕性之證，卽基於前節內之(13)與(18)二式，及　$1+e^{i\pi}=0$　　(19)

設如 π 爲代數的，則 $i\pi$ 亦然，卽爲有理係數

的代數式之根了。今試取其三次式，而假定其根爲 y_1, y_2, y_3，則 $i\pi$ 必在內。

但因(19)，可得　$(1+e^{y_1})(1+e^{y_2})(1+e^{y_3})=0$,

而 $1+(e^{y_1}+e^{y_2}+e^{y_3})+(e^{y_1+y_2}+e^{y_2+y_3}+e^{y_3+y_1})$

$$+e^{y_1+y_2+y_3}=0 \tag{20}$$

今欲證明此式之不可能。

y_1, y_2, y_3 之相稱函數，由假設(1)是有理數，故 y_1, y_2, y_3 爲有理代數式 $\phi(x)=0$ 之根。y_1+y_2, y_2+y_3, y_3+y_1 者亦然，故爲 $\phi_1(x)=0$ 之根。仿此，$y_1+y_2+y_3$ 爲 $\phi_2(x)=0$ 之根。故

$$\phi(x)\phi_1(x)\phi_2(x) \tag{21}$$

爲 x 之整函數，而當 x 取 y_j, y_j+y_k 或 $y_1+y_2+y_3$ 中一值時卽成0。但其中有的或者爲0，例如有 N 個。因此我們可剔出因子 x^N，而使(21)等於0，則得一方程 $\theta(x)=0$，幷可化其係數爲整者。0根旣挑出，$\theta(0)\neq 0$，故可寫 $\theta(x)$ 作

$$\theta(x)=ax^m+a_1x^{m-1}+a_2x^{m-2}+\cdots+a_m=0,$$

於此 a, a_1, a_m 爲整的，a 與 a_m 非0，a 幷是正的。

此式不難改變其形作$\theta_1(z)=z^m+b_1z^{m-1}+b_2z^{m-2}+\cdots b_m=0$ (22)

這裏係數爲整者，最高乘方者爲 1。設 $\theta(x)=0$ 之根爲 $x_1, x_2, x_3, \cdots$，此卽是 $y_j, y_j+y_k, y_1+y_2+y_3$ 中非爲0的數目。由(20)，可知必

$$K+e^{x_1}+e^{x_2}+e^{x_3}+\cdots=0 \qquad (23)$$

今於(13)內x處依次代入 $x_1, x_2, x_3, \cdots$而加之，則用(23)可得 $K\cdot F(0)+F(x_1)+F(x_2)+\cdots+\psi(x_1)+\psi(x_2)+\cdots=0$ (24)

我們倘若證明此式不可能，則卽知 π 之非代數數目了。欲證此，則可證

(1) $K\cdot F(0)+F(x_1)+\cdots$爲整數非爲0；以及

(2) $\psi(x_1)+\psi(x_2)+\cdots$之絕對値$<1$。

蓋如是則(24)卽不能成立。

我們可先設p爲質數，而 $f(x)=\dfrac{z^{p-1}[\theta_1(z)]^p}{(p-1)!}=\dfrac{a^{mp-1}x^{p-1}[\theta(x)]^p}{(p-1)!}$ (25)

蓋因 $\theta_1(z)$係用 a^{m-1} 乘 $\theta(x)$幷設 $z=ax$ 而得者。

將 $[\theta_1(z)]^p$ 展之，$[\theta_1(z)]^p = A_0 + A_1 z + A_2 z^2 + \cdots = A_0 + A_1 \alpha x + A_2 \alpha^2 x^2 + \cdots$，於此諸 A 為整數，而由(22)，$A_0 = b_m^p$，故非0。由(25)

$$f(x) = \frac{A_0 \alpha^{p-1} x^{p-1} + A_1 \alpha^p x^p + A_2 \alpha^{p+1} x^{p+1} + \cdots}{(p-1)!} \quad (26)$$

取其引生，設$x=0$，得

$f(0)=0$，$f'(0)=0, \cdots$，$f^{(p-2)}(0)=0$，$f^{(p-1)}(0) = A_0 \alpha^{p-1} = b_m^p \alpha^{p-1}$，$f^{(p)}(0) = pA_1 \alpha^p$，$f^{(p+1)}(0) = p(p+1) A_2 \alpha^{p+1}, \cdots$

今若如是選擇 p，使其大於最大的數目 α, b_m, K，則 $f^{(p-1)}(0)$ 不能為p除，而其他則或為0或可為 p 除。照(4)，可知$F(0)$為整數不能用 p 除者，$K \cdot F(0)$亦然。

(22)係用$z=\alpha x$，故今可使 $f(x)$ 作此形式：

$$f(x) = \frac{(z-z_k)^p B_1(z_k) + (z-z_k)^{p+1} B_2(z_k) + \cdots}{(p-1)!} =$$

$$\frac{\alpha^p (x-x_k)^p B_1(z_k) + \alpha^{p+1} (x-x_k)^{p+1} B_2(z_k) + \cdots}{(p-1)!} \quad (27)$$

於此 Z_k 為(22)之一根，$B_1(z_k), B_2(z_k), \cdots$ 為 z_k

之整函數，係數爲有理的。故如前，得

$$f(x_k)=0,\ f'(x_k)=0,\ f''(x_k)=0,\cdots,$$

$$f^{(p-1)}(x_k)=0,\ f^{(p)}(x_k)=pa^pB_1(z_k),\ f^{(p+1)}(x_k)$$
$$=p(p+1)a^{p+1}B_2(z_k),\cdots$$

倘設 $Q(z_k)=a^pB_1(z_k)+(p+1)a^{p+1}B_2(z_k)+\cdots,$

則由(4)

得 $$F(x_k)=pQ(z_k) \tag{28}$$

故 $$F(x_1)+F(x_2)+F(x_3)+\cdots=p[Q(z_1)+Q(z_2)+\cdots] \tag{29}$$

但此式之右端乃是(22)之根之整相稱函數，故必整的，有 p 爲因子。幷前者之結果，可知 $K\cdot F(0)+F(x_1)+F(x_2)+\cdots$ 爲一整數不能用 p 除，故非是0，而(1)已證明。

今證其(2)。將 $\theta(x)$ 寫作

$$\theta(x)=a(x-x_1)(x-x_2)\cdots(x-x_m) \tag{30}$$

則由(25)，得

$$f(x)=\frac{a^{(m+1)p-1}x^{p-1}(x-x_1)^p(x-x_2)^p\cdots(x-x_m)^p}{(p-1)!} \tag{31}$$

仍設 $|x|=X$，而 $|x_k|=X_k$，可知(31)內之係數不能大於

$$\frac{a^{(m+1)p-1}x^{p-1}(x+X_1)^p(x+X_2)^p\cdots(x+X_m)^p}{(p-1)!}$$

內者。今設 $P(X)=a^{m+1}X(X+X_1)(X+X_2)\cdots(X+X_m)$，則於任何 X，得

$$\frac{X^{p-1}[(X+1)(X+2)(X+3)]^p}{(p-1)!}<\frac{[P(X)]^p}{aX(p-1)!}=$$

$$\frac{P(X)}{aX}\cdot\frac{[P(X)]^{p-1}}{(p-1)!}。$$

今可如(18)從事，對於 X 之任何值，可選相當大的 p，俾

$$\frac{X^{p-1}[(X+1)(X+2)(X+3)]^p}{(p-1)!}$$

至隨意的小。由(18)，$\psi(x)$ 可任意小，因之，$\psi(x_1)+\psi(x_2)+\cdots$ 之絕對值可使之小於 1，祇要相當選擇 p 便行；如所欲證者。

如是，π 之超絕性已明了。